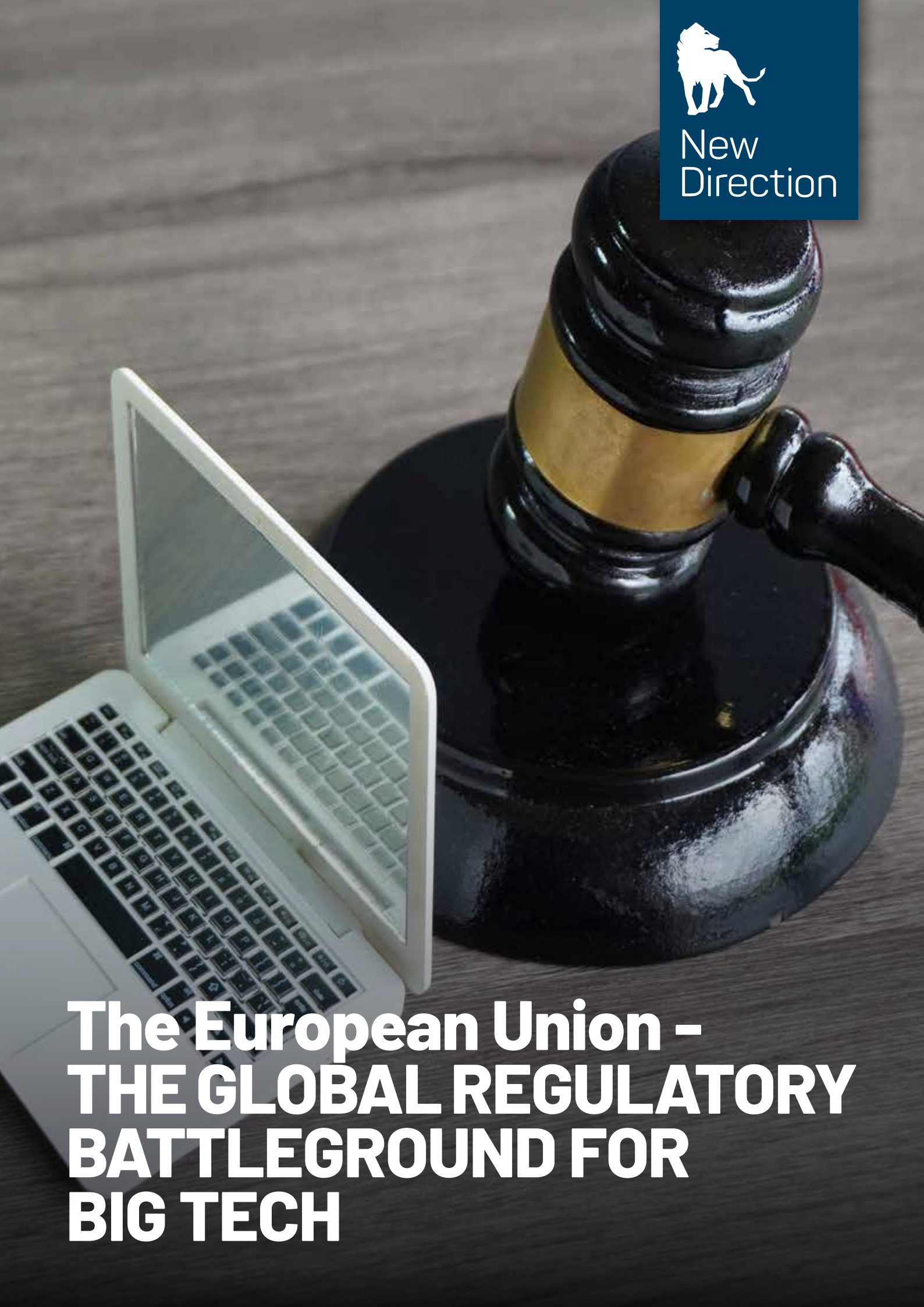
New Direction



The European Union – THE GLOBAL REGULATORY BATTLEGROUND FOR BIG TECH

New Direction

Founded by Margaret Thatcher in 2009 as the intellectual hub of European Conservativism, New Direction has established academic networks across Europe and research partnerships throughout the world.

newdirection.online @europeanreform

New Direction is registered in Belgium as a not-for-profit organisation and is partly funded by the European Parliament.
REGISTERED OFFICE: Rue du Trône, 4, 1000 Brussels, Belgium. EXECUTIVE DIRECTOR: Witold de Chevilly.

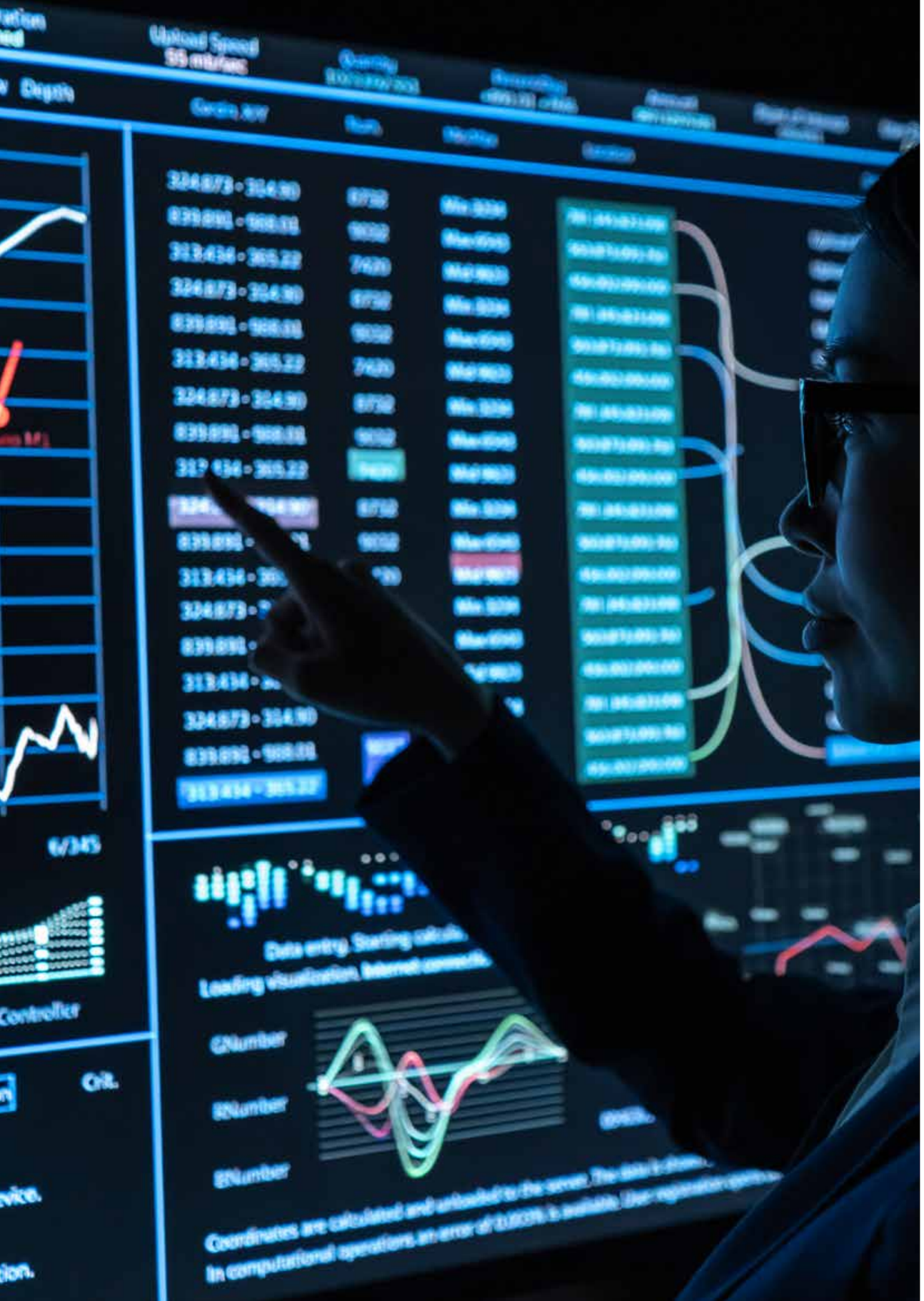
CONTENTS

EXECUTIVE SUMMARY

This report analyses how the European Union has become a crucial (and global) battleground for Big Tech companies. The report firstly analyses, the European Union has become the most powerful and most stringent regulator of Big Techs and of the digital economy, as a result of diverse policy imperatives such as integration of the European Single Market, protecting EU citizens' fundamental rights, preserving democracy, ensuring a fair and competitive social market economy, and more recently, geopolitical considerations such as preserving Europe's strategic autonomy and digital sovereignty. All these imperatives have led the EU to enact a complex and comprehensive web of legislation and regulations governing the Digital Economy.

However, as the report shows, the EU has become a *global* battleground because these regulations transcend EU borders. As the report analyses, the 'Brussels Effect' has enabled the EU to export its regulatory model (at first as an unintended consequence of market forces but increasingly as a conscious geopolitical decision), and this has meant that the regulatory developments that take place in the European Union don't only shape development for Big Techs in the EU itself, but also have an impact an impact on companies and governments around the world. This report will analyse the dynamics behind the 'Brussels Effect', and the global impact of the EU's digital regulatory framework.

From the starting point of these dynamics, the report will provide a detailed analysis of the key legislation and regulations that the European Union has enacted in the digital sphere, the obligations they have imposed on Big Techs, and the regulatory battles that have developed between the EU and Big Techs as a result of the EU's efforts to enforce these regulations and Big Tech companies' attempts to fight back against the obligations and costs imposed.



1

INTRODUCTION

The rapid **digital transformation** that Europe and much of the world have undergone has had profound **socioeconomic consequeneces**.[1] In this context of digital and technological transformation, **the European Union has been actively seeking to set the global regulatory standards for the technology industry**, via the so-called "**Brussels Effect**", which as section 2 of the report explains, enables the EU to export its regulatory standards abroad.[1 2] In the last year, the EU has passed several **key pieces of legislation**, such as the Digital Markets Act, the Digital Services Act, or the Chips Act, among others, and it is working to approve other rules such as the AI Act.

At the same time, the EU has been working to develop and implement a policy of **Strategic Autonomy** in order to reduce its dependence on third countries, as a response to the increasingly volatile geopolitical context, marked by geopolitical confrontation between the USA and China, and the protectionist policies of the USA.

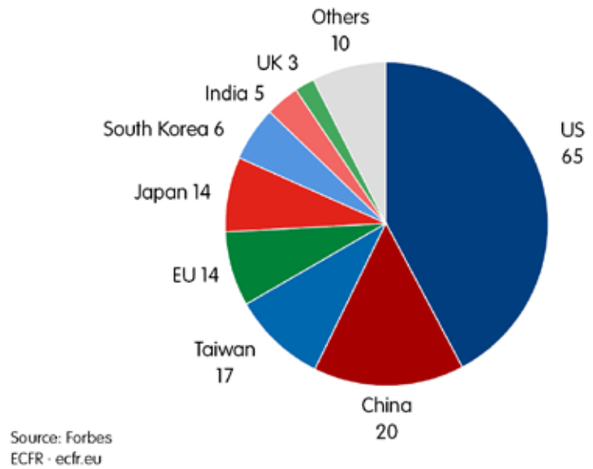
Therefore, **Big Tech companies**, largely American and Chinese, face a **new political and regulatory context** which will foreseeably have profound consequences for their businesses. In this context, the present report will analyse the recent and future regulatory developments in the digital field in the European Union, their impact on the industry, and how companies are responding. The present report analyses these important questions, and is structured as follows:

In the next section (**section 2**), the report will firstly analyse the **European Union's regulatory context**, as a backdrop to the analysis of specific regulations. This section will analyse the **ideological underpinnings of the European regulatory model**, namely promoting the integration of the Single Market, upholding citizens' fundamental rights, preserving democracy, and promoting a fair and competitive social market economy. As the report will explain, the EU has developed a distinctive "**rights-based regulatory model**", which at the heart of it is concerned about regulating Big Tech so that the digital economy is compatible with European citizens' individual and collective rights.[1] As *The Economist* puts it, "the EU is pioneering a distinct tech doctrine that aims to give individuals control over their own information and the profits from it, and to prise open tech firms to competition. If the doctrine works, it could benefit millions of users, boost the economy and constrain tech giants that have gathered immense power without a commensurate sense of responsibility".[3]

However, as section 2 of the report will also show, there are **geopolitical considerations that are increasingly shaping the European Union's regulatory approach**. Anu Bradford, a leading scholar on the EU's regulatory power and digital regulation, has characterised the digital economy as comprising three dominant digital powers, or "digital empires", namely the USA, China, and the European Union, who have developed distinct and "competing regulatory models" for governing their respective digital economies, based on distinct ideological commitments. Indeed, the three regulatory models "collide in the international domain" due to the digital empires' "mutual contest for influence" and efforts to "export their regulatory models to other countries" and "**shape the global digital order**".

What is most remarkable about the EU's status as a digital power, however, is the fact that **Europe lacks any significant Big Tech companies of its own**, and is instead reliant on mainly American and Chinese companies for providing services in the digital economy.[4 5] In fact, many Big Tech companies are dependent on the EU market, with Facebook, for instance, having more users in Europe than in the USA.[2] Furthermore, **the five main Big Tech giants (Alphabet, Amazon, Apple, Facebook and Microsoft) make on average 25% of their sales in the EU market**. This poses challenges for the EU, and will act as a barrier in Europe's efforts to achieve digital sovereignty.[5] Though as *The Economist* argues, this also has upsides, as the EU's regulators "are less captured by lobbying than America's and its courts have a more up-to-date view of the economy. Europe's lack of tech firms helps it take a more objective stance".[3]

Location of the world's largest tech companies [4]



Furthermore, despite this disadvantage, as the report will show, this lack of EU Big Tech companies hasn't hindered the EU's global influence in the digital economy. While the USA influences the digital economy through the huge "private power" of its Big Tech companies, and China through its vast "infrastructure power", the EU has been able to wield enormous influence through its vast "**regulatory power**". The EU has been able to export its regulatory power via the "**Brussels Effect**" and has therefore cemented itself as the **most powerful regulator** of the digital economy, as section 2 of the report will explain.[1]

Therefore, the **two important geopolitical dynamics shaping the European Union's regulatory approach** that section 2 analyses are the growing global influence of the European Union's regulatory model via the Brussels Effect, and the growing salience of concepts like "strategic autonomy" and "digital sovereignty" in the EU's policymaking in light of the increasingly volatile and fragmented global geopolitical context.

After analysing the regulatory context, **section 3** of the report will proceed to an in-depth analysis of the **EU's regulatory framework** governing the digital economy. This section will outline the broad objectives and policy guidelines governing the EU's regulatory approach, before surveying the main pieces of legislation and policy. Within this broad survey, the report will analyse in depth **six specific pieces of legislation** that are of particular importance for Big Techs and the Digital economy: the General Data Protection Regulation, the Digital Services Act, the Digital Markets Act, the Data Governance Act, the Chips Act, and the Cybersecurity Directive. This section will close with an analysis of important **future regulatory developments**, including the upcoming AI Act, the Data Act, and the Cyber Resilience Act.

After this detailed analysis of regulations and legislation in the EU, **section 4** of the report will finally analyse in detail the **specific regulatory battles between the EU and Big Tech**, and how these have played out, as a result of the EU's regulatory framework.

2

THE EUROPEAN UNION'S REGULATORY CONTEXT

This next section turns to the main focus of the report, which is regulation of Big Tech and the digital economy in the European Union. Understanding this topic is of paramount importance because, for various reasons that will be analysed by this report, over the past decade the European Union has asserted itself as the "**most powerful regulator of the digital economy**", **extending its influence globally to set the rules and standards that govern the digital economy, and acting as a first mover in the regulatory sphere**.[1]

Therefore, analysing and understanding the European Union's regulation of Big Tech and the digital economy is essential for policymakers and businesses alike, not just because of the weight of the EU Single Market in the digital economy, but because of the **global reach of EU regulations**. Before the detailed, in-depth analysis of the relevant key regulations in section 3, this proceeding section first provides an **overview of the European regulatory model**, and the different **ideological and policy imperatives** that underpin this model.

2.1 THE EU'S APPROACH TO BIG TECH REGULATION: EUROPEAN INTEGRATION AND RIGHTS

As Anu Bradford cogently argues in her book on 'Digital Empires',[1] the European Union has developed a distinct and characteristic "**European rights-driven regulatory model**", which unlike the other two major competing regulatory models, the American and Chinese models, views "**governments as having a central role in both steering the digital economy and in using regulatory intervention to uphold the fundamental rights of individuals, preserve the democratic structures of society, and ensure a fair distribution of benefits in the digital economy**".

First and foremost, the main motivation that has driven EU efforts to regulate and rein in big tech is the growing global concern about the **growing concentration of economic, political and cultural power that Big Tech companies have accrued**, and the **risks and potentially harmful effects** that are associated with this concentration of power.[1] These concerns have been exacerbated by scandals involving Big Tech and the use of private data by governments and private actors alike, such as the 2013 Snowden Revelations,[6] or the 2018 Cambridge Analytica scandal,[7] to name a few.

In this regard, especially in the last decade, there has been a "**backlash**" against the "**internet freedom agenda**" that the USA has championed, as concerns have grown about the **consequences of an unregulated Big Tech sector**, such as the **huge power that Big Tech companies have amassed** through their possession of personal data and their control over conversations on social media, the commercial advantage that this power gives them and their dominant market position, "**surveillance capitalism**" and the **exploitation of personal data** by both government and private actors, harmful online and disinformation as well as content moderation decisions, the ramifications of algorithms, the impact of digital platforms on democracy, and also concerns about the **dominance of the digital economy by American Big Tech firms** (further explored in subsection 3.2 on geopolitical concerns).[1 2 8]

As a response to these concerns, **the European Union has been "leading this fight" to "reclaim control over the industry"**. It has not been alone in its efforts to rein in Big Tech, but, as a manifestation of its "affinity with regulation", the EU has certainly been a first mover and has asserted itself as **the most powerful regulator**, setting the **most stringent regulations** and often determining the global rules and standards.[1]

In terms of the principles that underpin the European Union's rights-based approach to regulating Big Tech and the digital economy, Anu Bradford argues that the European Union has developed a "**European digital constitution**" over the last decade that is based on **four pillars**: **fundamental rights, democracy, fairness and redistribution, and the Digital Single Market**.[9] Another complementary way of conceptualising Europe's regulatory model employed by Bradford is that the **European Union's regulatory approach is underpinned by two imperatives or a "dual objective"**: firstly, the **integration of the EU Single Market** (which corresponds to the fourth pillar of the "digital constitution"), and secondly, the European Union's policy imperatives and ideological commitment to promote European values and "**enhance the individual and collective rights of European citizens in a digital society**" (the first, second and third pillars of the "digital constitution".[1]

The first of the two imperatives that has traditionally been the main initial driver of the European Union's regulation of the digital economy has been the **integration of the EU Single Market**, with the objective of harmonising Member States' regulatory frameworks, removing barriers to trade within the EU, preventing the fragmentation of the Single Market, and creating a Digital Single Market. Therefore, the "EU's regulatory agenda for the digital economy is directly woven into the overarching governing objective of advancing European integration by creating a single market", and indeed, the integration of the Single Market has provided the "**legal basis**" for EU regulations in many domains which aren't exclusive competences of the EU, including the digital economy.[1 2] In fact, according to a 2019 paper by the McKinsey Global Institute, an important factor that has hindered the **emergence of European Big Tech actors to rival American and Chinese companies** is the continued **fragmentation of the European market** despite efforts to build a Digital Single Market.[10] This echoes the Commission's 'A Digital Agenda for Europe' communication presented in 2010, which evaluated that "persistent fragmentation is stifling Europe's competitiveness in the digital economy".[11]

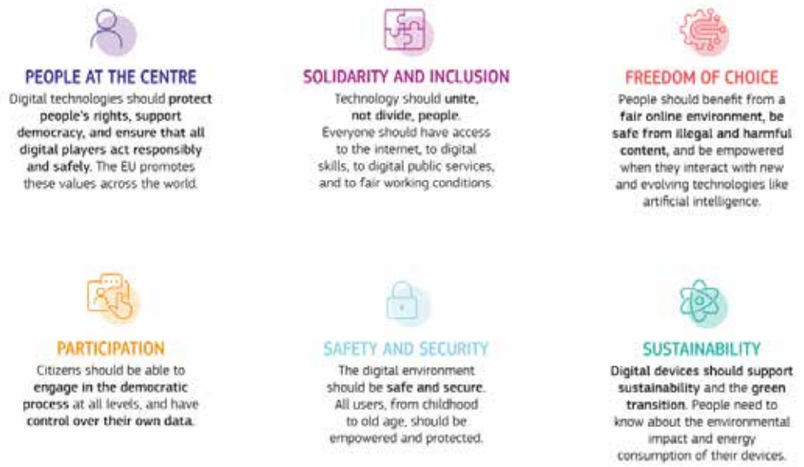
Therefore, many of the EU's most prominent and far-reaching **regulations** affecting Big Tech and the digital economy are **justified on the legal basis of the integration of the Single Market**. For instance, the Digital Markets Act (DMA) asserts that the measures adopted at a national level to address the unfair practices of 'gatekeepers' has "created divergent regulatory solutions which results in the **fragmentation of the internal market**". Therefore, the rules that the DMA establishes on "contestability and fairness for the markets in the digital sector" are justified under the basis that they seek to "**facilitate cross-border business** within the Union and thereby improve the proper functioning of the internal market, and to eliminate existing or likely emerging fragmentation in the specific areas covered by this Regulation".[12] Similarly, the EU's upcoming and groundbreaking AI Act that is in the works offers as a legal basis the fact that the Proposal for a Regulation seeks to "ensure the proper functioning of the internal market by setting **harmonised rules**" for AI, because the "emerging patchwork of potentially divergent national rules" could lead to the "fragmentation of the internal market on essential elements regarding in particular the requirements for the AI products and services, their marketing, their use, the liability and the supervision by public authorities", as well as "the substantial diminishment of **legal certainty** for both providers and users of AI systems on how existing and new rules will apply to those systems in the Union".[21]

However, the EU's regulatory approach has another even more important imperative which is the **promotion of rights**. As Bradford puts it, fundamental rights are "deeply entrenched in the ethos of the EU" and they form a **"value-based constitutional foundation for European integration" that guides legislative activity in areas including the digital economy**.[1] Especially so in the last decade, the **growing dominance of Big Tech companies** and the associated risks perceived by governments has led to an "**ideological shift**" in the EU, whereby the **protection of rights and market-**correcting principles have gained more weight in the regulation of the digital economy *vis a vis* the Single Market imperative. Therefore, EU regulations, including in the digital domain, now pursue a "**dual objective**" of integrating the Single Market while safeguarding Europeans' rights.[1]

As outlined above, within this second broad imperative relating to the protection of European citizens' individual and collective rights, **three main pillars** can be identified. All in all, the European Union follows a regulatory model that views the government as having a "central role" in regulating the digital economy, employing "regulatory intervention" to uphold the three-rights based pillars of the EU digital constitution: **upholding individuals' fundamental rights, preserving society's democratic structures, and ensuring a fair distribution of the benefits of the digital economy**.[1] Or, as the Commission itself put it in its communication 'Shaping Europe's Digital Decade', the three key objectives that the Commission sets out for the digital transformation are "**technology that works for people**", "**a fair and competitive economy**", and "**an open, democratic and sustainable society**".[13]

For example, the **European Declaration on Digital Rights and Principles for the Digital Decade**, adopted by the European Commission, Parliament and Council in December 2022, affirms that the EU is a "union of values" founded on "respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights", and that in this regard, "**the digital transformation should not entail the regression of rights**". In this regard, the Declaration asserts that "**people are at the centre of the digital transformation** in the European Union. Technology should serve and benefit all people living in the EU and empower them to pursue their aspirations, in full security and respect for their fundamental rights", as well as to strengthen the "democratic functioning of the digital society and economy".[14]

Main principles of the 'European Declaration on Digital Rights and Principles'



Source: European Commission

In terms of the first pillar of the "European digital constitution", namely the **upholding of fundamental rights**, prominent EU policymakers have highlighted the importance of upholding fundamental rights in regulating the digital economy. For instance, in 2021, the Executive Vice-President of the European Commission for a Europe fit for the Digital Age, Margrethe Vestager, and the High Representative of the European Union for Foreign Affairs and Security Policy, Josep Borrell, highlighted the importance of a "more **human-centric digital transformation** that maximizes the benefits of technology and minimises the risks it poses", and that the "digital revolution lives up to" the fundamental rights enshrined by the 1948 Universal Declaration of Human Rights, such as "the dignity of the individual, the right to privacy and to non-discrimination, and the freedoms of speech and belief".[15]

Therefore, the EU's regulation of many aspects of the digital economy and Big Tech like data protection, artificial intelligence (AI) and content moderation have been **strongly anchored to these fundamental rights-based concerns**.[1] Regarding the first, the European Union has been very active in regulating the digital economy to uphold **the right to privacy and the protection of personal data**, seeking to protect these from "exploitation by governments or private companies alike" through regulations such as the **General Data Protection Regulation** (GDPR, which is analysed in detail in section 4).[16] Regarding the implications of AI for fundamental rights, the EU has also been active in regulating **to mitigate the potential rights-based risks associated with unregulated AI**. For instance, in 2019 the Commission published 'The Ethics Guidelines for Trustworthy AI',[17] and in 2021 it proposed a new groundbreaking Regulation, the **AI Act**, which will likely be approved this year and is analysed in detail in section 4.[18] Finally, regarding online content moderation, the EU has been active in regulating Big Tech to ensure that **content moderation decisions** balance the right to freedom of expression with the protection of human dignity and other rights, covering issues such as hate speech or non-discrimination.[1] In this regard, the EU's regulatory activity has also been groundbreaking with its **Digital Services Act** (DSA) passed in 2022 to regulate the online platforms' content (analysed in detail in section 4).[21]

Turning to the second pillar of the EU's digital constitution, regarding the use of regulations to **preserve society's democratic structures**, the EU has been active in regulating Big Tech and the digital economy to **protect democratic institutions and discourse**.[1] For example, as section 4 will detail, the aforementioned **DSA** addresses the **systemic risks** posed to democracy and society by online disinformation. Furthermore, in 2021 the European Commission presented a **Proposal for a Regulation on the transparency and targeting of political advertising**,[22] which seeks to protect electoral integrity by mandating the labelling of political advertisements and restricting targeting and amplification techniques. In the related sphere of strengthening the free and pluralistic media, the EU has passed laws such as the **2019 Copyright Directive**, which among other aspects, seeks to ensure fairer remuneration for creators and rightsholders, press publishers and journalists when their works are used online, as well as to increase transparency in their relationships with online platform.[23]

Finally, the third pillar of the rights-based regulatory approach of the EU is **promoting fairness and redistribution in the digital economy through regulation**, which is related to the EU's **ideological commitment to a social market economy**. In this sphere, the EU has pursued regulatory and supervisory action, usually targeting American Big Tech companies, to **ensure a level playing field in the digital**

economy, to **prevent power from being concentrated** in a few Big Tech companies, and to **redistribute the gains from the digital transformation** more evenly.[1] The regulatory actions undertaken, which are analysed in detail in section 3 on the regulatory framework section and 4 on battles between the EU and Big Tech companies, includes the Commission's **competition policy decisions** to ensure a level playing field, the **Digital Markets Act** which is an *ex ante* regulation on competition, state aid policies, or the digital levy proposed by the Commission in 2020.

2.2 GEOPOLITICAL CONSIDERATIONS SHAPING THE EU'S REGULATORY APPROACH

The Brussels Effect

However, aside from the two traditional imperatives that have underpinned the European Union's regulatory approach, namely integration of the Single Market and protection of European citizens' individual and collective rights; **in the last decade the European Union's regulatory activity has also acquired an important geopolitical dimension**, which means that an analysis of the EU regulatory model is incomplete without proceeding to analyse it with a global perspective. Specifically, there are **two important geopolitical dimensions to the EU's regulation of the digital economy and Big Tech** that this next subsection examines: firstly, the **global influence of the European Union's regulation** through the so-called **'Brussels Effect'**, and secondly, the growing importance of considerations about **'strategic autonomy'** in the volatile geopolitical context.

Regarding the first, through its regulatory action, the European Union doesn't only safeguard the fundamental rights of its own citizens or rein in Big Techs in Europe, but rather, **EU regulatory action transcends its own boundaries and shapes the global digital economy** through the **'Brussels Effect'**. This term, which was coined by Bradford, refers to the European Union's "**unilateral power to regulate the global marketplace**".[1,2] Through the 'Brussels Effect', the EU is able to "**transform the world towards its norms simply by regulating the European single market**". In fact, through the 'Brussels Effect', the EU's **regulatory power** has become the **main source of the EU's global influence** in shaping the digital economy, enabling the EU to export its regulatory model and to become the "primary source" of legal norms, rules and standards that shape the digital economy across borders; and to be considered one of the 3 "**digital empires**" along with the USA and China despite the EU's comparative lack of tech giants.[1]

As Bradford argues, the Brussels Effect is transmitted by via two mechanisms: the ***de facto*** and ***de jure*** **Brussels Effect**. The *de facto* Brussels Effect takes place when market forces incentivise multinational companies to adapt their global production or business practices to comply with EU regulations. The **five preconditions** for this mechanism to develop, which are generally present in the digital economy, are the following:[1,2]

- The **EU's large and attractive consumer market**, which is highly valuable to Big Tech companies, and which therefore induces regulatory compliance by companies.
- The **EU's regulatory capacity** through its strong, competent institutions that are able to promulgate regulations and enforce compliance.
- The EU's preference for **stringent regulations**, as a result of citizens' and institutions' ideological preference for a social market economy and regulatory intervention (relative to other countries' like the US' more free-market oriented policies).
- The regulation of **inelastic targets** such as consumer markets or data, which are those that cannot be moved to other jurisdictions to circumvent EU regulations. In these cases, it is the location of the consumer, rather than the producer, that determines the application of EU regulations.
- **Non-divisibility** of the regulatory targets, which is when companies have an economic incentive to standardise, as opposed to customise, their production or business practices across jurisdictions to conform to the most stringent regulatory standard (usually the EU's) across global operations.

In turn, the ***de jure*** **Brussels Effect** usually follows the *de facto* Brussels Effect, and takes place when foreign companies, after having changed their practices to comply with EU regulations, **lobby the government of their domestic jurisdictions** to adopt EU-style regulations at home so as to not be at a competitive disadvantage against their domestic competitors.

The reason why the Brussels Effect is important is that despite the fact that the EU lacks any Big Tech actors, **the Brussels Effect enables the EU to "harness the power of foreign companies"**, in this case largely US Big Tech companies, **to export its regulatory model and influence the digital economy**. By simply regulating its own Single Market, the EU has been able to "**transform global markets towards its norms**" in the digital sphere and "**globalise the European rights-based regulatory model**" in a way that the USA and China are unable to do, with its regulatory influence having a tangible impact both on Big Tech companies' business practices, as well as on foreign governments' legislative activities. In fact, there is a growing trend whereby democratic governments around the world are shifting towards this European regulatory model in their efforts to rein in Big Tech companies while using government intervention to build a fairer, more human-centric digital economy.[1]

Most importantly from a geopolitical perspective, **the EU is becoming increasingly aware of the global influence that the 'Brussels Effect' awards it,** and is therefore increasingly complementing its internal regulatory imperatives with **external motivations, such as shaping the global regulatory environment and pursuing global influence** (for both **economic reasons** like protecting the competitiveness of European industry, and for **normative reasons** like promoting its model of governance).[2] Indeed, in its 2007 working document on 'The external dimension of the single market review', the European Commission recognised that "**the EU is emerging as a global rule maker**, with the single market framework and the wider EU economic and social model increasingly serving as a reference point", and consequently recognised that there is a "window of opportunity" for the EU to "take a lead" in "**promoting its modern regulatory framework internationally**".[24] Similarly, in the 2007 policy paper 'A single market for citizens', the Commission asserted that the development of EU regulations gives the bloc "**the potential to shape global norms** and to ensure that fair rules are applied to worldwide trade and investment", characterising the single market ad a "launch pad of an ambitious global agenda".[25]

Specifically to the digital economy, in its 2010 communication on 'A comprehensive approach on personal data protection in the European Union', the European Commission pointed out that "a high and uniform level of data protection within the EU will be the best way of **endorsing and promoting EU data protection standards globally**", and further argued that "the European Union must remain a **driving force behind the development and promotion of international legal and technical standards for three protection of personal data**".[26] More recently, in its 2020 communication 'Shaping Europe's Digital Future', the European Commission asserted that "**the EU should leverage its regulatory power**, reinforced industrial and technological capabilities, diplomatic strengths and external financial instruments to **advance the European approach and shape global interactions**".[13] Furthermore, the President of the European Commission Ursula von der Leyen stated herself in the 2020 State of the Union address that "**Europe must now lead the way on digital – or it will have to follow the way of others, who are setting these standards for us**".[27] Similarly, in her 2023 State of the Union address, von der Leyen stated that in responding to challenges of the digital economy such as "disinformation, spread of harmful content, risks to the privacy of our data ... and a breach of our fundamental rights", Europe has become "the **global pioneer of citizens' rights** in the digital world".[28]

Furthermore, as Bradford argues, in the volatile geopolitical context characterised by an **absence of American leadership** as well as the **rise of Asian powers** (explored in detail in the next subsection), has provided the EU with additional incentives **to assume the role of a "global standard setter"**, as well as to seek to "cement its rules globally" while it has the power to do so.[2]

There are many global examples of the impact of the Brussels Effect, whereby foreign governments and Big Tech companies alike have adopted elements of the EU's regulatory model. The EU's **GDPR** provides clear examples of the Brussels Effect. Following the adoption of the GDPR in 2018, the US state of **California** adopted the California Privacy Rights Act (**CPRA**), closely modelled on the GDPR.[1] As far as private companies are concerned, that same year Meta's CEO Mark **Zuckerberg** argued in favour of a "**common global framework**" of privacy regulation, "rather than regulation that varies significantly by country and state" so as to prevent the fragmentation of the Internet and uniform protection of privacy rights. And in advocating for a "common global framework", it was precisely European standards that Zuckerberg defended, arguing that "it would be good for the Internet if more countries adopted regulations such as **GDPR as a common framework**".[29]

On other policy issues like competition policy and content moderation, the UK provides a cogent example. Despite Brexit, the **UK** has undertaken legislative **efforts to regulate Big Tech** in parallel to the EU, and has introduced two Bills that are similar in scope to the DSA and the DMA (and arguably more stringent in some respects)[1]: the **Online Safety Act** (passed in October 2023),[30] and the **Digital Markets, Competition and Consumers Bill** (presented in April 2023).[31,32]

Furthermore, the increasingly important policy issue of **Artificial Intelligence** will likely be "**the next frontier of the Brussels Effect**", and indeed the European Union has been a "**first mover**" and is "taking a lead in regulating artificial intelligence. As section 3 analyses, the EU has formulated regulatory proposal for an ambitious and comprehensive AI Act,[18] which is the world's first comprehensive AI law.[19,18]

However, in line with the 'Brussels Effect'**, other states have followed the EU's lead and are beginning efforts to also regulate AI**. Most remarkable is the example of the United States. At the end of October 2023, US President Joe Biden issued an **Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence**, which, despite the US's traditionally free market-oriented approach to Big Tech regulation, establishes objectives that are in line with the EU's human-centric and risks-based AI regulatory approach[1] (which is detailed in the analysis of the AI Act in section 3). For example, the Executive Order establishes **new standards for AI safety and security**, requiring developers of the most powerful AI systems share their safety test results and other critical information with the US government, provides for the development of standards, tools, and tests to help ensure that AI systems are safe, secure, and trustworthy; and foresees the establishment of standards and best practices for detecting AI-generated content and authenticating official content.[20] Furthermore, as Bradford argues, AI developers around the world will likely have economic and reputational incentives to extend the EU's stringent AI standards across all their global markets.[1]

Strategic Autonomy

The geopolitical considerations that have just been analysed are arguably outward-looking in their nature. However, the second important geopolitical imperative that must be analysed is more inward-looking, and it concerns the fact that, in the **increasingly volatile geopolitical context of the recent years, the concept of strategic autonomy has been gaining ground in many policy domains in the European Union**, ranging from defence, to industry, to the digital economy, while other countries like the USA and China have also increasingly adopted more **economically nationalist and protectionist policies**. As this subsection will show, strategic autonomy concerns have in turn **affected the EU's approach to regulating Big Tech and the digital economy**, adding a new layer of complexity to the regulatory model.

In essence, recent global developments such as the protectionist **'America First'** policies of the Trump Presidency (and the continuation of some of them under Biden's Presidency), **China's growing assertiveness** and its **geopolitical competition with the USA**, and more recently the **COVID-19 pandemic, supply chain shocks, and the war in Ukraine**, have pushed the EU to acknowledge **the risk posed by supply chain disruptions** and to **reevaluate its dependence** on third countries for the supply of certain essential goods, raw materials and services; as well as to seek to **rebalance economic openness with security** in order for the EU to be able to **act autonomously in strategically important policy areas** in the increasingly volatile geopolitical context.[33] [34] Consequently, as EU High Representative Josep Borrell has argued, "strategic autonomy is more salient than ever" because the pandemic exposed the "asymmetrical nature of interdependence, and the vulnerability of Europe", while "**science, technology, trade, data, and investments are becoming sources and instruments of force in international politics**".[35]

Along the same lines, in a speech delivered in in November 2023 reflecting on EU-China relations, the European Commissioner for Internal Market, Thierry Breton, stated that "with the COVID-19 pandemic, Russia's war of aggression in Ukraine, the conflict in the Middle East, the energy crisis, supply crunches and attempts to destabilise our democracies, we have seen the **emergence of a more assertive Europe that looks after its own interests**" and which has "realised that it needs to **rebalance its relationship** with China, as with others". In this regard, Commissioner Breton emphasised the importance, from the EU's perspective, of "**de-risking our economies and societies**", which "is not politically motivated or protectionist", but "follows the same rationale that China or the US have been pursuing for years: **increase the resilience of the economy and boost industrial and technological competitiveness**". As Breton starkly put it, "whenever the security interests of Europe will be at stake, Europe will not hesitate to act on its own. **Europe will be an actor if its own security, and not a mere follower of the decision of others**".[36]

The digital economy is no exception to this emerging imperative of strategic autonomy. Indeed, the pandemic and its consequences highlighted the **pervasiveness of the digital transformation** in all aspects of society, as well as the need to **reduce dependencies in key technology areas, supply chains, and critical infrastructures**.[37] Therefore, as Bradford argues, in this increasingly "**contested geopolitical environment**", governments are veering towards what she calls "**techno-nationalism**", including all three major digital powers, the USA, China and the EU.[1] **Questions about who produces the technologies of the future, who owns them, and who regulates them are becoming central to geopolitical competition**, as "digital empires" compete for global influence in the digital economy and to **reap the economic and geopolitical benefits** that flow form it.[1] [5] In a nutshell, "digital competition is no longer just about economics".[9]

There have been various international and geopolitical challenges trends that have affected the global digital economy and the European Union. Firstly, the **growing technological competition between the USA and China**, which is one dimension of the broader geopolitical rivalry. As part of the **US-China tech rivalry**, in order to preserve its technological lead over China, the USA has engaged in actions like **export controls** of strategic technologies such as semiconductors, banning Chinese investments in key digital infrastructure, and unprecedented **government funding into strategic technologies** like AI and semiconductors. President Trump engaged in trade wars against China (and indeed also the EU) and promoted protectionist policies, but even Biden's Presidency has promoted **protectionist policies** and an **industrial policy** approach, injecting unprecedented amounts of money into the domestic economy.[1]

Examples include the **2021 Infrastructure Investment and Jobs Act**, which Biden argued aimed to "boost America's innovative edge in markets where global leadership is up for grabs – markets like battery technology, biotechnology, computer chips, clean energy, the competition with China in particular" and for which the President claimed "not a contract will go out to a company that is not an American company with American products, all the way down the line, and American workers".[38] More recently, Congress passed the **Inflation Reduction Act (IRA) in 2022**, which many EU leaders have interpreted as "protectionism in disguise".[39]

The knock-on effect of this US-China tech rivalry and their respective protectionist policies is that they have **fuelled subsidy races and "techno-nationalist" impulses around the world, including in the European Union**.[1] Essentially, the US-China tech rivalry has "**caught Europe in the crossfire**" [5] as a result of the **EU's dependence on both the USA and China for digital services and technologies**, which in turn has exposed the **vulnerability** of the EU to the **decisions made by other states**, and has given rise to the concept of "**digital sovereignty**" as a means to ensure the **EU's capacity to act autonomously**, defend its interests, and reevaluate and manage their dependencies.[1] [5] In fact, as will be analysed in greater depth in section 4 on regulatory battles between the EU and US Big Techs, these concerns about excessive dependence on US Big Tech companies may have also arguably **influenced the EU's regulatory actions against American Big Techs**, including imposing digital taxation or fining large American technology companies for anti-competitive practices.[2] [5]

With regard to China, the EU's concerns have also been related to the **Chinese state's practices**, but **national security** has also been an important factor due to **China's growing assertiveness**. The EU's External Action service argues that the EU-China relationship has "deteriorated", such that China is now defined as an "**economic competitor and a systemic rival**".[40] Indeed, in the digital sphere, China's rising influence and economic weight has further increased the EU's sense of vulnerability and **perceived threat to its digital sovereignty**.[1] [5] Especially so at a time when China is "increasingly interested in the European market" and "**challenging European companies in virtually every high-technology sector**,[9] while China is also actively seeking to **expand its authoritarian digital model** and wield its vast infrastructure power via the "**Digital Silk Road**".[1] [41] The EU's strategic autonomy concerns in relation to China also have a **national security dimension**. For example, the European Union has faced growing concerns about the potential threat that relying on **Huawei** as a provider for their **5G network** poses to national security, fearing exposure to **Chinese government surveillance**,[1] and indeed, some sources claim the EU may be considering a ban on Member States using companies that are deemed to present a security threat for their 5G networks.[42]

More on the economic front, the EU's concerns also stem from **China's unfair trade practices**. As Commissioner for Internal Market, **Thierry Breton,** stated in a speech in Beijing in November 2023, "**competition needs to take place on fair and reciprocal terms**, not by dumping products on markets, keeping prices artificially low with state subsidies, or favouring domestic manufacturers over European operators", citing the EU's recently launched "anti-subsidies investigation into electric vehicles coming from China to establish whether anticompetitive behaviour is taking place", or the solar industry, where "China's massive economies of scale ... has led to extreme overcapacity of solar photovoltaic modules in Europe".[36]

Therefore, in this **contested geopolitical context**, the European Union has become "more conscious of its need to **build its technological capabilities and to reduce its dependencies**", thus introducing the **new dimension of "digital sovereignty" into its policymaking**.[1] In essence, the European Union has become increasingly aware of the need to maintain its **capacity to act autonomously in the digital realm and to defend its interests**.[9] In its 2020 communication 'Shaping Europe's Digital Future', the European Commission emphasised the importance of "technological sovereignty" to guarantee "**Europe's ability to define its own rules and values in the digital age**" as well as to "**reduce our dependency** on other parts of the globe for the most crucial technologies". As such, "**technological sovereignty**" is understood as "ensuring the **integrity and resilience** of our data infrastructure, networks and communications".[13] More recently, in their March 2022 Versailles Declaration, EU leaders addressed the importance of "building our European sovereignty", with one of the key pillars being "reducing our strategic dependencies" in key "sensitive areas" related to the digital economy such as semiconductors, artificial intelligence, or Cloud and 5G deployment.[43]

High-level EU leaders have further emphasised the importance of strategic autonomy in the digital sphere. In her 2021 State of the Union address, Commission President **Ursula von der Leyen** highlighted the "importance of **investing in our European tech sovereignty**", and stressed that the EU has to "double down" on investment in order to "shape our digital transformation according to our own rules and values". As von der Leyen highlighted, citing the example of semiconductors, "Europe's share across the entire value chain ... has shrunk. We depend on state-of-the-art **chips manufactured in Asia**. So this is not just a matter of our competitiveness. This is also a matter of **tech sovereignty**".[44] More recently, von der Leyen starkly defended the importance of European digital sovereignty in her 2023 State of the Union address. As von der Leyen asserted, "European companies also need **access to key technologies to innovate, develop and manufacture**. This is a question of European sovereignty ... it is an **economic and national security imperative to preserve a European edge** on critical and emerging technologies.[28]

Along the same lines, in his November 2023 speech on EU-China relations, **Thierry Breton** stated that in line with the imperative of "**de-risking our economies and societies**" to "**increase the resilience** of the economy and boost **industrial and technological competitiveness**", the European Union has "identified 10 strategic technologies which deserve specific attention", including "advanced semiconductor technologies, Artificial Intelligence technologies, Quantum technologies, and biotechnologies", and that the EU will consequently "take appropriate measures" such as "diversification of supply, increased partnerships, strengthened investment or more protective measures, such as export controls or reciprocity measures".[36]

Therefore, these important geopolitical considerations that incorporate concerns about national security, have played an **increasing role in the European Union's regulatory activity**, as is manifested in its policy outputs. For example, in July 2023 the European Union adopted the **Chips Act**, which, as section 3 analyses in detail, establishes measures to ensure the EU's security of supply, resilience and technological leadership in semiconductor technologies and applications, strengthen manufacturing activities in the Union, stimulate the European design ecosystem, and support scale-up and innovation across the whole value chain.[45] More recently, in October 2023, the European Commission presented a '**Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States**', in

which the Commission identifies 4 technology areas, namely **Advanced Semiconductors**, **Artificial Intelligence**, **Quantum Technologies** and **Biotechnologies**, which it considers that present the "most sensitive and immediate risks related to technology security and technology leakage".[46] The Commission therefore recommends that these technology areas be subject to a collective risk assessment with Member States by the end of the year should, as a "matter of highest priority". The objective of the risk assessment is to identify and analyse vulnerabilities of a systemic nature according to their potential impact on the EU's economic security and the degree of likelihood that the negative impact materialises.

Additionally, the EU has increasingly been promoting **industrial policy** initiatives to boost **Europe's technological capabilities** and shed its foreign dependencies.[1] One notable example is the European Commission's June 2023 proposal to create a **Strategic Technologies for Europe Platform** (STEP) as a "structural answer to the investment needs of the EU's industries".[47] In this regard, the STEP was conceived with the objective of supporting the development and manufacturing of critical technologies, including digital technologies, through mobilising funds from existing EU programmes like Horizon Europe or the Recovery and Resilience Facility, as well as a proposed additional €10 billion.

Therefore, as this subsection has shown, growing geopolitical tensions have led governments, including the EU, to increasingly **view digital regulation through the lens of geopolitics and national security**, which in turn has led them to avoid protectionist and nationalist policies to boost their own technological capabilities and self-sufficiency.[1] The EU faces an important challenge in this regard, in so far as it must reconcile the liberal impulses of the single market with the new struggle over digital sovereignty,[9] all the while incentivising innovation.

3

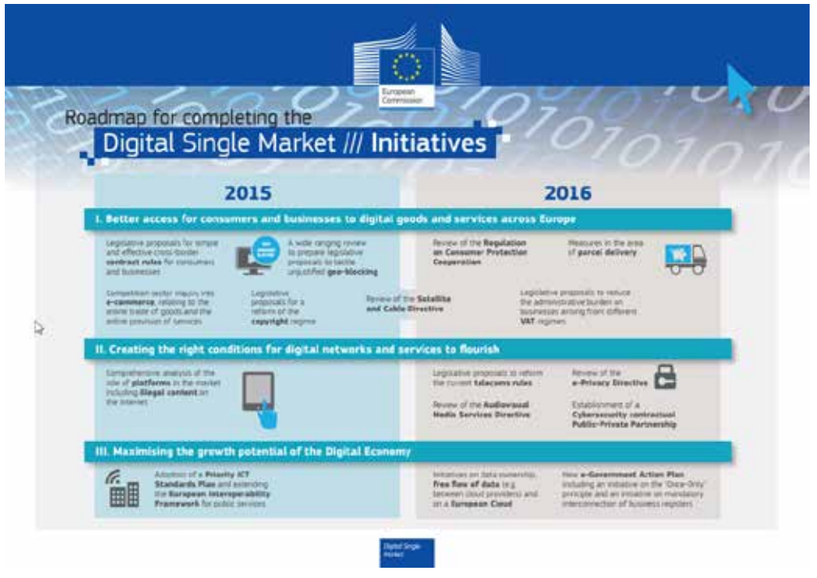
THE EUROPEAN UNION'S REGULATORY FRAMEWORK

This next section proceeds to analyse in detail the **main pieces of legislation and regulations** that form the basis of the European Union's regulatory framework governing the digital economy and Big Tech, before the final section if this report which analyses the regulatory battles between the EU and Big Tech companies.

3.1 THE REGULATORY FRAMEWORK

The first major milestone in the European Union's regulation of the digital economy was arguably the **Digital Single Markt Strategy**, presented in May 2015 by the **Juncker** Commission (2014-2019).[48] This Strategy had the objective of building a Digital Single Market, addressing "fragmentation and barriers that do not exist in the physical Single Market" so as to create economic opportunities for the EU and enable it to "lead in the global digital economy". In this regard, the Digital Single Market Strategy established three **fundamental pillars for the Digital Single Market** and set out a roadmap. The three pillars were:

1. **Better access** for consumers and businesses to **online goods and services** across Europe – this required the rapid removal of key differences between the online and offline worlds to break down barriers to cross-border online activity.
2. Creating the **right conditions for digital networks and services to flourish** – this required high-speed, secure and trustworthy infrastructures and content services, supported by the right regulatory conditions for innovation, investment, fair competition and a level playing field.
3. Maximising the **growth potential of our European Digital Economy** – this required investment in ICT infrastructures and technologies such as Cloud computing and Big Data, and research and innovation to boost industrial competitiveness as well as better public services, inclusiveness and skills.



Source: European Commission

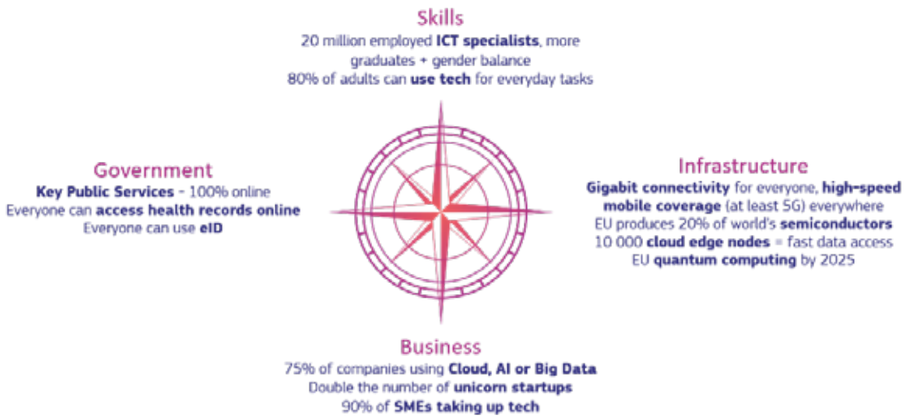
More recently, one of the **six key priorities** that the **von der Leyen** Commission (2019-2024) established in its political guidelines was building "**a Europe fit for the digital age**".[49]

Further to this aim, in September 2021 the European Commission presented the Proposal for a Decision establishing the **2030 Policy Programme "Path to a Digital Decade"**,[50] approved by the Council and Parliament and adopted in December 2022.

The Policy Programme established "**general objectives**" for the European Union's regulatory activity in the digital sphere, forming the basis for the specific pieces of legislation that have been proposed in this period. The "general objectives" include the following:

- Promoting a **human-centred, fundamental-rights-based, inclusive, transparent, and open digital environment** where secure and interoperable digital technologies and services observe and enhance EU principles, rights and values and are accessible to all, everywhere in the EU.
- Reinforcing Member States' **collective resilience** and bridging the **digital divide**, developing basic and advanced digital skills and competencies, and fostering the development of high-performing digital capacities within horizontal education and training systems.
- Ensuring the EU's **digital sovereignty** in an open manner, in particular by secure and accessible digital and data infrastructures capable of efficiently storing, transmitting and processing vast volumes of data that enable other technological developments, supporting the competitiveness and sustainability of the EU's industry and economy, and the resilience of the EU's value chains, as well as fostering the start-up ecosystem and the smooth functioning of the European digital innovation hubs.
- Developing a comprehensive and sustainable ecosystem of **interoperable digital infrastructures**, where high performance, edge, cloud, quantum computing, artificial intelligence, data management and network connectivity work in convergence, to promote their uptake by businesses in the EU, and to create opportunities for growth and jobs through research, development and innovation, and ensuring that the Union has a competitive, secure and sustainable data cloud infrastructure in place, with high security and privacy standards and complying with the Union data protection rules.
- Promoting an EU digital regulatory environment to support the ability of **EU undertakings**, especially that of **SMEs**, to compete fairly along global value chains.
- Ensuring that **online participation in democratic life** is possible for everyone, and that public services, health and care services are also accessible in a trusted and secure online environment for everyone.
- Ensuring that digital infrastructure and technologies, including their supply chains, become more **sustainable, resilient, and energy- and resource-efficient**.
- Facilitating fair and non-discriminatory conditions for users during the digital transformation throughout the EU by strengthening the **synergies between private and public investments** and the use of EU and national funds, and by developing predictable regulatory and supportive approaches that also involve the regional and local levels.
- Improving **resilience to cyberattacks**, contributing to increasing risk-awareness and the knowledge of cybersecurity processes, and increasing the efforts of public and private organisations to achieve at least basic levels of cybersecurity.

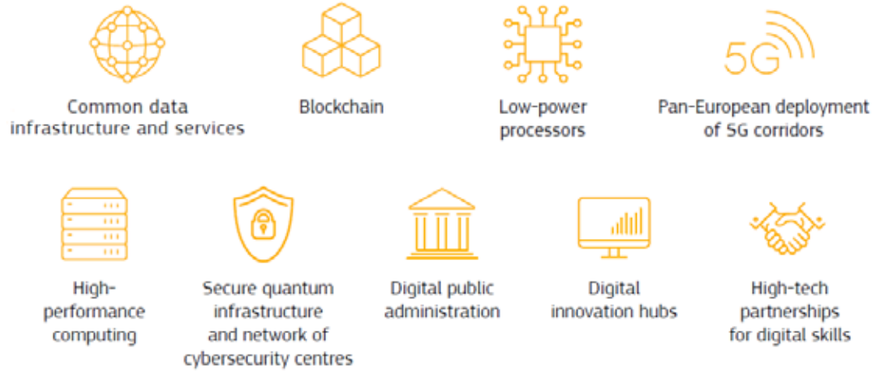
Apart from the "general objectives", the Policy Programme also establishes specific **targets**, **grouped around 4 areas**:



Source: European Commission

The Policy Programme also establishes that the EU may undertake "**multi-country projects**" to improve cooperation in achieving the "general objectives", including to improve cooperation, reinforce the EU's technological excellence, leadership, innovation and industrial competitiveness in critical technologies and infrastructures, or to address strategic vulnerabilities and dependencies.

Multi-country programmes may receive contributions from EU programmes and investment schemes (including the pandemic Recovery and Resilience Facility). The initial list of areas that the Commission has identified for multi-country projects includes the following:



Source: European Commission

3.2 EU LEGISLATION ON THE DIGITAL ECONOMY

On the basis of this overarching policy framework, the European Union has been very **active in regulating Big Techs and enacting new regulations to govern the digital economy**. In 2022, the Directorate-General for Internal Policies of the European Commission produced a report, at the request of the European Parliament's Artificial Intelligence in a Digital Age (AIDA) Committee, which provided an overview of all existing and planned EU legislation in the digital field.[51] As the report highlights, the EU has established a very **comprehensive legislative framework** governing diverse aspects of the digital economy and Big Tech.

The report identified **48 legislative acts and proposals**, grouped around seven policy domains, which are summarised in the tables below. The policies identified include regulations, directives, legislative proposals, as well as Commission regulations, alliances and treaties. Furthermore, the report considers policies which are in force, as well as draft proposals and proposals that have been announced. The **seven policy domains** into which the legislation is classified are: A) ICT services, infrastructure, networks; B) trust and security; C) consumer protection and competition; D) online services and e-commerce; E) data protection and governance; F) copyright and audio-visuals; and G) e-Government.

The colouring of the cells indicates the following: blue is legislation that is in force, light blue is legislative proposals, green is announced legislative acts, and orange is alliances and treaties.

ICT services, infrastructure, networks

- Council Regulation (EU) 2021/1173 of 13 July 2021 on establishing the European High Performance Computing Joint Undertaking and repealing Regulation (EU) 2018/1488
- Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast)
- Directive 2014/61/EU of the European Parliament and of the Council of 15 May 2014 on measures to reduce the cost of deploying high-speed electronic communications networks Text with EEA relevance (under revision)
- Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres
- Regulation (EU) 2023/588 of the European parliament and of the Council of 15 March 2023 establishing the Union Secure Connectivity Programme for the period 2023-2027 ('infrastructure for Resilience, Interconnection and Security by Satellite'- IRIS²)

- Regulation (EU) 2023/1781 of the European Parliament and of the Council of 13 September 2023 establishing a framework of measures for strengthening Europe's semiconductor ecosystem and amending Regulation (EU) 2021/694 (Chips Act)
- Proposal for a Regulation of the European Parliament and the Council on a pilot regime for market infrastructures based on distributed ledger technology
- Industrial Alliance on Processors and Semiconductor Technologies
- EU-US Trade and Technology Council

Trust and security

- Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (under revision)
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
- Proposal for a Regulation of the European Parliament and the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts
- Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148
- Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)
- Proposal for a Regulation of the European Parliament and of the Council on machinery products
- Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014
- Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Cyber Resilience Act)

Consumer protection and competition

- Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services
- Regulation (EU) 2022/612 of the European Parliament and of the Council of 6 April 2022 on roaming on public mobile communications networks within the Union (recast)
- Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union
- Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)
- Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937
- Commission Regulation (EU) 2023/1670 of 16 June 2023 laying down ecodesign requirements for smartphones, mobile phones other than smartphones, cordless phones and slate tablets pursuant to Directive 2009/125/EC of the European Parliament and of the Council and amending Commission Regulation (EU) 2023/826
- Proposal for a Directive of the European Parliament and of the Council amending Directive 2014/53/EU on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment
- Legislative proposal on multimodal digital mobility services

Online services and e-commerce

- EU VAT for e-commerce package (EU VOEC)
- Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC
- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')
- Regulation (EU) 2018/302 of the European Parliament and of the Council of 28 February 2018 on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC
- Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act)
- Legislative proposal for the creation of a Single Market Emergency Instrument

Data protection and governance

- Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast)
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
- Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union
- Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services
- Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)
- Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act)
- Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space
- European Alliance for Industrial Data, Edge and Cloud.

Copyrights and audio-visuals

- Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC
- Directive (EU) 2019/789 of the European Parliament and of the Council of 17 April 2019 laying down rules on the exercise of copyright and related rights applicable to certain online transmissions of broadcasting organisations and retransmissions of television and radio programmes, and amending Council Directive 93/83/EEC
- Regulation (EU) 2017/1128 of the European Parliament and of the Council of 14 June 2017 on cross-border portability of online content services in the internal market
- Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC
- Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases (under revision)

e-Government

- Directive 2014/55/EU of the European Parliament and of the Council of 16 April 2014 on electronic invoicing in public procurement
- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (under revision)
- Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EC) No 767/2008, (EC) No 810/2009 and (EU) 2017/2226 of the European Parliament and of the Council, Council

Regulations (EC) No 1683/95, (EC) No 333/2002, (EC) No 693/2003 and (EC) No 694/2003 and Convention implementing the Schengen Agreement, as regards the digitalisation of the visa procedure

Although this non-exhaustive list of legislation and proposals is in itself complex and extensive, there are arguably **8 key pieces of legislation** within the list that form the **backbone of the EU's regulatory framework on the digital economy**, and which have a particular significance from the point of view of Big Techs. These pieces of legislation were mentioned in the broad discussion about the EU's regulatory approach in section 2, but this next subsection analyses each of these pieces of legislation in detail. The regulations and directives in question are the following:

- The General Data Protection Regulation (**GDPR**)
- The Digital Services Act (**DSA**)
- The Digital Markets Act (**DMA**)
- The European Data Governance Act (**DGA**)
- The **Chips Act**
- The Directive on measures for a high common level of cybersecurity across the Union (**NIS2 Directive**)
- The next subsection after that one will also addresses three important future regulations:
  - The **Data Act**
  - The Artificial Intelligence Act (**AI Act**)
  - The **Cyber Resilience Act**

The General Regulation on Data Protection (GDPR)

The General Data Protection Regulation (**GDPR**) [16] [51] [52] has been in force since May **2018**. The GDPR is a **data privacy and security law** that seeks to **give EU citizens to better control over their personal data** by facilitating citizen access, providing an individual the right to know when their personal data has been hacked, and providing rules on the right to erasure of personal data from platforms. Additionally, it harmonises rules to reduce excessive bureaucracy and allow business to benefit from greater consumer trust. It also establishes the data protection officer role, which is responsible for data protection and is designated by public authorities and businesses which process data on a large scale.

The GDPR is widely considered the **strongest privacy and security law in the world**, and as section 3 explained, has become a global "**gold standard**"[1] that is replicated abroad on how to protect individuals' personal data from exploitation, both from governments or private companies. Indeed, the GDPR calls for the application of principles such as **lawfulness, fairness and transparency in the processing of personal data**, **purpose limitation** in personal data collection, as well as **data minimisation**, and **integrity and confidentiality** in data processing. Furthermore, the Act creates new rights and obligations such as the accountability of data controllers, the "**right to be forgotten**", or "**privacy by design**" requirements.

In terms of the specific provisions of the GDPR, the regulation lists the rights of the data subject (the rights of the individuals whose personal data is being processed). These strengthened rights give individuals more control over their personal data, including through:

- the need for an individual's **clear consent** to the processing of their personal data.
- **easier access** for the data subject to their personal data.
- the **right to rectification**, to **erasure** and '**to be forgotten'**.
- the **right to object**, including to the use of personal data for the purposes of 'profiling'.
- the **right to data portability** from one service provider to another.

Source: Council of the European Union.

The GDPR also establishes the **obligation for controllers** (those who are responsible for the processing of data) to provide **transparent and easily accessible information** to individuals on the processing of their data, as well as the obligations for those processing personal data on their behalf (processors).

- These include the **obligation to implement appropriate security measures**, according to the risk involved in the data processing operations they perform.
- Controllers are also required in certain cases to provide **notification of personal data breaches**. All public authorities and those companies that perform certain risky data processing operations will also need to appoint a data protection officer.

Source: Council of the European Union.

In terms of the application of the data protection rules, the GDPR confirms the existing obligation for member states to establish an **independent supervisory authority** at national level and establishes a mechanism to **create consistency in the application of data protection law** across the EU.

- The GDPR establishes that a single supervisory decision is taken in cross-border cases where several national supervisory authorities are involved. This principle, known as the **'one-stop-shop' principle**, means that a company with subsidiaries in several member states will only have to deal with the data protection authority in the member state of its main establishment.
- In turn, the **European Data Protection Board** makes sure that the GDPR is fully applied. This board consists of representatives of all 27 independent supervisory authorities.
- They have the right to have a decision by their data protection authority reviewed by their national court, irrespective of the member state in which the data controller concerned is established.

- **Severe sanctions** are provided for against controllers or processors who violate data protection rules. Data controllers can face fines of up to €20 million or 4% of their global annual turnover.

Finally, the GDPR also covers **transfers of personal data** to non-EU countries and international organisations.

- The European Commission is in charge of **assessing the level of protection given by a territory or processing sector** in a non-EU country.
- Where the Commission has not taken an **adequacy decision** on a territory or sector, transfer of personal data may still take place in particular cases or when there are **appropriate safeguards** in place.

The Digital Services Act (DSA) and the Digital Markets Act (DMA)

The Digital Services Act (**DSA**) and the Digital Markets Act (**DMA**) are two landmark pieces of legislation that were jointly submitted by the European Commission to the European Parliament and the Council as a **package in December 2020**. Together, the DSA and DMA seek to create a safer digital space in which the fundamental rights of all users of digital services are protected, and to establish a level playing field to foster innovation, growth, and competitiveness, both in the European Single Market and globally. The DSA and the DMA were approved by the European Parliament in July 2022 and the Council in October 2022, and the two regulations **came into force in November 2022**.[51][53]

The Digital Services Act (DSA)

The overarching objective of the Digital Services Act [21][54][55][56] is to create a **safer online environment for digital users and companies, protect fundamental rights in the digital space**, and the legitimate interests of all parties involved, particularly EU citizens. In this regard, the DSA seeks to establish a **comprehensive and legally binding transparency and accountability regime to make digital companies accountable for the content posted on their platforms**.[1]

To sum up, the DSA establishes **harmonised rules for intermediary services** with the objective of ensuring a **safe, predictable and trusted online environment**, addressing the dissemination of **illegal content online** and the **societal risks** that the dissemination of disinformation or other content may generate, and within which **fundamental rights** enshrined in the Charter are effectively protected and innovation is facilitated. The objective is to "rebalance" the "responsibilities of users, platforms, and public authorities according to European values, placing citizens at the centre", guaranteeing:

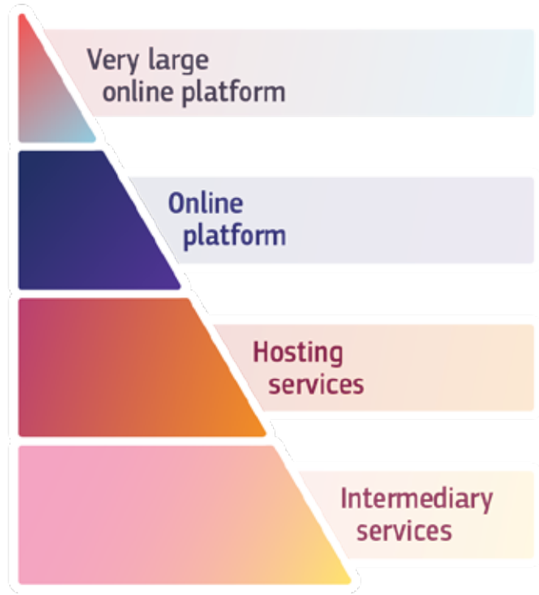
- better **protection of fundamental rights**, more **control and choice**, stronger protection of children online, and less exposure to **illegal content** for **citizens**.
- **legal certainty**, **harmonisation** of rules, and greater ease to start-up and scale-up in Europe for **providers of digital services**.
- access to EU-wide markets through platforms, and level-playing field against providers of illegal content for **business users of digital services**.
- greater **democratic control and oversight** over systemic platforms, and **mitigation of systemic risks**, such as manipulation or disinformation for **society at large**.

For these purposes, the DSA establishes a series of **rules that must be followed by all online intermediary companies** that connect users with content, products and services in the EU single market, whether they are established inside or outside the Union, to better protect users and enhance transparency. These include:

- **Measures to counter illegal content online**, including illegal goods and services. The DSA imposes new mechanisms allowing users to flag illegal content online, and for platforms to cooperate with specialised 'trusted flaggers' to identify and remove illegal content.
- **New rules to trace sellers on online marketplaces**, to help build trust and go after scammers more easily; a new obligation by online marketplaces to randomly check against existing databases whether products or services on their sites are compliant; sustained efforts to enhance the traceability of products through advanced technological solutions.
- **Effective safeguards for users**, including the possibility to challenge platforms' content moderation decisions based on a new obligatory information to users when their content gets removed or restricted.
- Wide ranging **transparency measures for online platforms**, including better information on terms and conditions, as well as transparency on the algorithms used for recommending content or products to users.
- **New obligations for the protection of minors** on any platform in the EU.
- **Obligations for very large online platforms and search engines** to prevent abuse of their systems by taking risk-based action, including oversight through independent audits of their risk management measures. Platforms must mitigate against risks such as disinformation or election manipulation, cyber violence against women, or harms to minors online. These measures must be carefully balanced against restrictions of freedom of expression, and are subject to independent audits.
- A new **crisis response mechanism** in cases of serious threat for public health and security crises, such as a pandemic or a war.
- **Bans on targeted advertising** on online platforms by profiling children or based on special categories of personal data such as ethnicity, political views or sexual orientation. Enhanced transparency for all advertising on online platforms and influencers' commercial communications.
- A ban on using so-called '**dark patterns'** on the interface of online platforms, referring to misleading tricks that manipulate users into choices they do not intend to make.
- New provisions to allow **access to data to researchers of key platforms**, in order to scrutinise how platforms work and how online risks evolve.
- **Users will have new rights**, including a right to complain to the platform, seek out-of-court settlements, complain to their national authority in their own language, or seek compensation for breaches of the rules. Representative organisations will also be able to defend user rights for large scale breaches of the law.
- **A unique oversight structure**. The Commission is the primary regulator for very large online platforms and very large online search engines (reaching 45 million users), while other platforms and search engines will be under the supervision of Member States where they are established. The Commission will have enforcement powers similar to those it has under anti-trust proceedings. An EU-wide cooperation mechanism will be established between national regulators and the Commission.
- The **liability rules for intermediaries** have been reconfirmed and updated by the co-legislator, including a Europe-wide prohibition of generalised monitoring obligations.

The rules established by the DSA cover a wide variety of digital platforms and online intermediary companies:

- **Very Large Online Platforms** pose particular risks in the dissemination of illegal content and societal harms. Specific rules are foreseen for platforms reaching more than 10% of 450 million consumers in Europe.
- **Online platforms** bringing together sellers and consumers such as online marketplaces, app stores, collaborative economy platforms and social media platforms.
- **Hosting services** such as cloud and webhosting services.
- **Intermediary services** offering network infrastructure: Internet access providers, domain name registrars.



Source: European Commission

Nonetheless, the rules established by the DSA are **proportionate to the companies' size and impact on society and the online ecosystem**. Therefore, while very small platforms are exempt from most obligations, stricter rules apply to very large online platforms (**VLOPs**) and search engines (**VLOSEs**) with more than 45 million active

users, considering the key role they play in e-commerce, in disseminating information and in facilitating the exchange of opinions and ideas.

For instance, these types of platforms have specific **due diligence obligations**, as they are obliged to "diligently identify, analyse and assess any **systemic risks** in the Union stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services", in relation to systemic risks such as the dissemination of illegal content, "negative effects for the exercise of fundamental rights", or "negative effects on civic discourse and electoral processes, and public security".

In this regard, the DSA requires the **risk assessment** to take into account factors such as **algorithmic systems and content moderation system**, and for the VLOPs and VLOSEs to "put in place reasonable, proportionate and effective **mitigation measures**, tailored to the specific systemic risks identified, with particular consideration to the impacts of such measures on fundamental rights".

The following table summarises the new obligations imposed by the DSA on the main types of platforms:

NEW OBLIGATIONS	INTERMEDIARY SERVICES	HOSTING SERVICES	ONLINE PLATFORMS	VERY LARGE PLATFORMS
Transparency reporting	X	X	X	X
Requirements on terms of service due account of fundamental rights	X	X	X	X
Cooperation with national authorities following orders	X	X	X	X
Points of contact and, where necessary, legal representative	X	X	X	X
Notice and action and obligation to provide information to users		X	X	X
Reporting criminal offences		X	X	X
Complaint and redress mechanism and out of court dispute settlement			X	X
Trusted flaggers			X	X
Measures against abusive notices and counter-notices			X	X
Special obligations for marketplaces, e.g. vetting credentials of third party suppliers ('KYBC'), compliance by design, random checks			X	X
Bans on targeted adverts to children and those based on special characteristics of users			X	X
Transparency of recommender systems			X	X
User-facing transparency of online advertising			X	X
Risk management obligations and crisis response				X
External & independent auditing, internal compliance function and public accountability				X
User choice not to have recommendations based on profiling				X
Data sharing with authorities and researchers				X
Codes of conduct				X
Crisis response cooperation				X

The DSA **came into force in November 2022**. The general date of entry into application of the DSA for all regulated entities and the deadline for Member States to establish **Digital Services Coordinators** (DSCs) to allow for the supervision and enforcement of the DSA is the is the 17th of **February 2024**. Following the entry into force, online platforms had 3 months (until February 2023) to report the number of active end users on their websites, which must now be updated **every 6 months**.

Based on the numbers published by the platforms and its investigative powers, the **European Commission** made the decision to **designate several platforms as VLOPs and VLOSEs in April 2023,** designating nineteen prominent Big Tech companies as VLOPs and VLOSEs, including Amazon, Facebook or Twitter in the first category, and Google Search in the second.[57] In the case of these platforms, then, they became regulated entities and were given 4 months (until the end of **August 2023**) to **comply with the obligations under the DSA**, including carrying out and providing the first annual risk assessment exercise.

Furthermore, in **April 2023**, the Commission launched the **European Centre for Algorithmic Transparency** (ECAT), a first-of-its-kind scientific centre which will support the Commission and national authorities in the monitoring of the application of the DSA. Among others, ECAT will:

- conduct technical tests on algorithmic systems to understand their functioning.
- analyse transparency reports, risk assessments and independent audits.
- support investigations and inspections.
- identify emerging risks associated with the use of VLOPs/VLOSEs.
- act as a knowledge hub for research conducted thanks to access to data provided by the DSA.

In terms of **enforcement**, companies that do not follow the DSA face penalties and fines proportionate to their size:

- companies with less than 45 million active users may get penalties, including fines, as laid down in member states' national laws.
- companies with more than 45 million active users may get fines of up to 6% of their global turnover.

The Digital Markets Act (DMA)

The Digital Markets Act [12 58] is a Regulation that aims to ensure the **proper functioning of the internal market** through harmonised rules to guarantee for all businesses contestable and fair markets in the digital sector where "**gatekeepers**" are present, to the benefit of business users and end users, to afford them **safeguards against unfair practices by "gatekeepers"**. As Bradford puts it, the DMA, unlike other *ex post* competition policy decisions from the Commission, is an "***ex ante* regulation on competition**", which seeks to ensure fair competition in the digital marketplace by regulating "gatekeepers".[1]

In this regard, the DMA sets out **rules for platforms that act as "gatekeepers"**, large platforms that have a durable position between business users and end users due to their impact on the digital markets. The DMA establishes a set of narrowly defined **objective criteria for qualifying** a large online platform as a so-called "**gatekeeper**", and a series of **obligations and prohibitions** that these platforms will have to comply with to ensure these platforms behave in a fair way online. Under the DMA, digital "gatekeepers" are defined as "undertakings providing core platform services", with three key criteria for their designation as such:

1. Have a **significant impact on the internal market**:
    - annual EU turnover equal to or above EUR 7,5 billion in each of the last three financial years,
    - average market capitalisation or its equivalent fair market value amounted to at least EUR 75 billion in the last financial year,
    - and it provides the same core platform service in at least three Member States
2. Provide a **core platform service which is an important gateway** for business users to each end users:
    - provides a core platform service that in the last financial year has at least 45 million monthly active end users established or located in the Union and at least 10 000 yearly active business users established in the Union
3. Enjoy an **entrenched and durable position**, in its operations, or it is foreseeable that it will enjoy such a position in the near future:
    - where the thresholds in point 2 were met in each of the last three financial years.

In turn, "core platform services" are defined as the following under the DSA:

- Online intermediary services.
- Online search engines.
- Online social networking services.
- Video-sharing platform services.
- Number-independent interpersonal communications services.
- Operating systems.
- Web browsers.
- Virtual assistants.
- Cloud computing services.
- Online advertising services.

The DSA establishes the following **obligations for "gatekeepers"**:

- **allowing end users to access and use**, through its core platform services, **content, subscriptions, features or other items**, by using the software application of a business user, including where those end users acquired such items from the relevant business user **without using the core platform services of the gatekeeper**.
- **allow and technically enable end users to easily un-install any software applications on the operating system of the gatekeeper**, without prejudice to the possibility for that gatekeeper to restrict such un-installation in relation to software applications that are essential for the functioning of the operating system or of the device and which cannot technically be offered on a standalone basis by third parties; and to easily change default settings on the operating system, virtual assistant and web browser of the gatekeeper that direct or steer end users to products or services provided by the gatekeeper.
- making the basic functionalities of its number-independent interpersonal communications services **interoperable** with the number-independent interpersonal communications services of another provider offering or intending to offer such services in the

Union, by providing the necessary technical interfaces or similar solutions that facilitate interoperability, upon request, and free of charge.

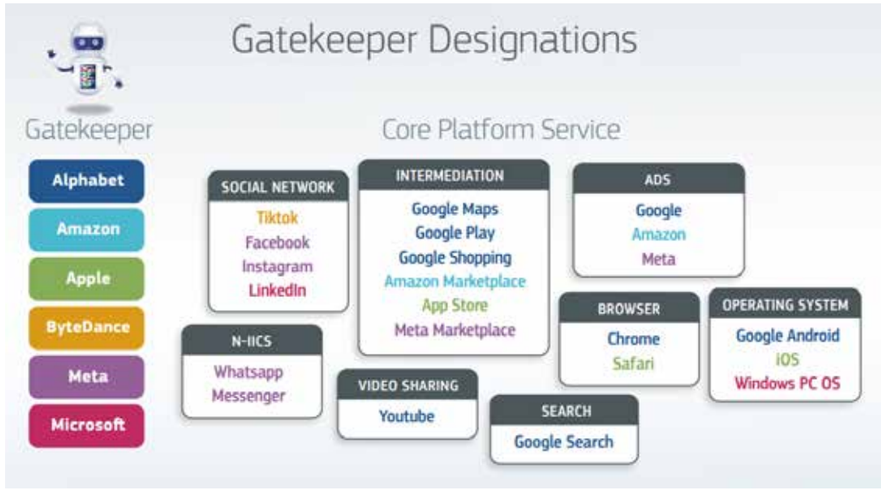
The DSA also sets out **prohibitions for "gatekeepers"**, such as:

- **processing**, for the purpose of providing online advertising services, **personal data of end users using services of third parties** that make use of core platform services of the gatekeeper.
- **combining personal data from the relevant core platform service** with personal data from any further core platform services or from any other services provided by the gatekeeper or with personal data from third-party services.
- **cross-using personal data from the relevant core platform** service in other services provided separately by the gatekeeper, including other core platform services, and vice versa.
- **signing in end users to other services of the gatekeeper** in order to combine personal data.
- **preventing business users from offering the same products or services to end users** through third-party online intermediation services or through their own direct online sales channel at prices or conditions that are different from those offered through the online intermediation services of the gatekeeper.
- **preventing or restricting business users or end users from raising any issue of non-compliance** with the relevant EU or national law by the gatekeeper with any relevant public authority, including national courts, related to any practice of the gatekeeper. This is without prejudice to the right of business users and gatekeepers to lay down in their agreements the terms of use of lawful complaints-handling mechanisms.
- requiring end users to use, or business users to use, to **offer**, or to **interoperate** with, an **identification service, a web browser engine or a payment service, or technical services** that support the provision of payment services, such as payment systems for in-app purchases, of that gatekeeper in the context of services provided by the business users using that gatekeeper's core platform services.
- **requiring business users or end users to subscribe to, or register with, any further core platform services** as a condition for being able to use, access, sign up for or registering with any of that gatekeeper's core platform services.
- **using, in competition with business users, any data that is not publicly available that is generated or provided by those business users** in the context of their use of the relevant core platform services or of the services provided together with, or in support of, the relevant core platform services, including data generated or provided by the customers of those business users.

To ensure that the new gatekeeper rules keep up with the fast pace of digital markets, the **Commission** will carry out **market investigations**, whereby the Commission will be able to:

- qualify companies as gatekeepers.
- update dynamically the obligations for gatekeepers when necessary.
- design remedies to tackle systematic infringements of the Digital Markets Act rules.

The **European Commission designated the first six "gatekeepers"** in **September 2023**, namely Alphabet, Amazon, Apple, ByteDance, Meta and Microsoft. These "gatekeepers" were given 6 months, until **March 2024**, to ensure that each of their **22 designated core platform services comply** with the obligations and prohibitions established under the DMA.[59]



Source: European Commission

In terms of **enforcement**, the fines for noncompliance are:

- up to 10% of the company's total worldwide annual turnover, or,
- up to 20% in the event of repeated infringements.
- In the event of systematic infringements of the DMA obligations by gatekeepers, additional remedies may be imposed on the gatekeepers after a market investigation. Such remedies will need to be proportionate to the offence committed. If necessary and as a last resort option, non-financial remedies can be imposed. These can include behavioural and structural remedies, e.g. the divestiture of (parts of) a business.

The Data Governance Act (DGA)

The Data Governance Act [60] [61] [62] [63] was presented by the European Commission in **November 2020**, as one of the two legislative initiatives under the '**European Strategy for data**' [64] a package that aims to **create a single market for data** to ensure the European Union's **global competitiveness and data sovereignty**. The other legislative initiative under the strategy, the proposed Data Act, hasn't been adopted yet and is analysed in the next subsection. The DGA **entered into force in June 2022**, and after a 15-month grace period, became applicable in September 2023.

The DGA is a cross-sectoral instrument that aims to **make more data available by regulating the re-use of publicly held, protected data**, by boosting data sharing through the regulation of novel data intermediaries and by encouraging the sharing of data for altruistic purposes. The public sector holds vast amounts of **protected data** that cannot be re-used as open data but that could be re-used under specific EU or national legislation.

Therefore, the DGA provides **rules and safeguards to facilitate the re-use of such data** whenever it is possible under other legislation, given that a **wealth of knowledge** can be extracted from such data without compromising its protected nature, and the fact that data-driven innovation can have enormous societal and economic benefits in many areas like healthcare, the environment or public administration.

For this purpose, the DGA regulates:

- **Conditions for the re-use**, within the EU, of certain categories of **data held by public sector bodies** (data protected on the grounds of commercial confidentiality, statistical confidentiality, the protection of intellectual property rights of third parties, or the protection of personal data):
  - **Public sector bodies** competent to grant or refuse access for the re-use of protected categories of data must make publicly available the **conditions** for allowing such re-use.
  - The conditions for re-use must be **non-discriminatory, transparent, proportionate and objectively justified**.
  - Public sector bodies must ensure that the **protected nature of the data is preserved**, and for that purpose they may provide for requirements like granting access for the re-use of data only once the data has been anonymised in the case of personal data, or modified, aggregated or treated by other methods of disclosure control in the case of commercially confidential information, as well as to ensure that the public sector body provides a secure processing environment for the access and re-use of the data.

- The right to re-use data may be granted to the extent necessary for the provision of a service or the supply of a product in the **general interest** that would not otherwise be possible, and the duration of an exclusive right to re-use data shall not exceed 12 months (or 30 months from the entry into force of the DGA for longer-term agreements that were in place before the Regulation's entry into force).

- The European Commission shall establish a **European single access point** offering a searchable electronic register of data available in the national single information points.

The DGA also establishes a **notification and supervisory framework** for the provision of **data intermediation services**, which are neutral third parties that connect individuals and companies that hold data with others that want to use data. The DGA establishes requirements for these services to ensure they function as trustworthy organisers of data sharing, establishing obligations such as:

- Complying with strict requirements to ensure neutrality and avoid conflicts of interest.

- Having structural separation from any other value-added services provided.

- Having price terms independent of whether a potential data holder or data user is using other services.

- Register with a competent authority.

- The DGA also establishes a **framework for voluntary registration of entities** which collect and process data made available for altruistic purposes (**data altruism**), which is when companies or individuals give their consent to make data that they generate available for use in the public interest, voluntarily and without reward.

  - The DGA establishes that the Commission shall establish a European data altruism consent form for the purpose of data collection based on data altruism, and that the Commission will maintain an EU-level register of organisations engaged in data altruism.

- The DGA also provides a framework for the establishment of a **European Data Innovation Board**, whose tasks include advising and assisting the Commission in:

  - developing consistent practice in processing requests for data reuse.

  - enhancing the interoperability of data and data-sharing services.

  - developing consistent practice of competent authorities in enforcing requirements applicable to data intermediation service providers.

- On **international data flows**, the DGA also establishes safeguards to protect data from unlawful access by non-EU states' authorities.

The Chips Act

The Chips Act [45] [65] [66] responds to the EU's **geopolitical considerations** about the continent's **overdependence on Asia for semiconductor manufacuring**.[1] As the Commission recognises, "semiconductors are the **essential building blocks of digital and digitised products**. From smartphones and cars, through critical applications and infrastructures for healthcare, energy, defence, communications and industrial automation, **semiconductors are central to the modern digital economy**". However, "they are also at the centre of strong **geostrategic interests** and the **global technological race**", and "the pandemic exposed a weakness in the ecosystem within both Europe and other regions in the world experiencing significant shortages of chips".

With that in mind, the European Union proposed the Chips Act in February of 2022, which "puts in place a comprehensive set of measures to ensure the **EU's security of supply, resilience and technological leadership in semiconductor technologies and applications**" and "reinforce" Europe's "capabilities in semiconductors to ensure future competitiveness and maintain its technological leadership and security of supply".

The Chips Act establishes a framework for **strengthening the EU's semiconductor sector based on three pillars**.

- **Pillar one** – establishment of the **Chips for Europe Initiative**:

  - The objective is to achieve **large-scale technological capacity building** and support related **research and innovation activities** throughout the EU's semiconductor value chain to enable development and deployment of cutting-edge semiconductor technologies, next-generation semiconductor technologies and cutting-edge quantum technologies and the innovation of established technologies that will reinforce advanced design, systems integration and chip production capabilities in the Union, thereby increasing the competitiveness of the EU.

  - The Initiative has **five operational objectives**:

    1. bilding up advanced design capacities for integrated semiconductor technologies.

    2. enhancing existing and developing new advanced pilot lines across the Union to enable development and deployment of cutting-edge semiconductor technologies and next-generation semiconductor technologies.

    3. building advanced technology and engineering capacities for accelerating the innovative development of cutting-edge quantum chips and associated semiconductor technologies.

    4. establishing a network of competence centres across the Union by enhancing existing or creating new facilities.

    5. undertaking activities ('Chips Fund' activities), to facilitate access to debt financing and equity, including by providing clear guidance, in particular for start-ups, scale-ups, SMEs and small mid-caps in the semiconductor value chain, through a blending facility under the InvestEU Fund and via the European Innovation Council.

  - The Initiative will be supported by **€3.3 billion of EU funds**, which is expected to be matched by funds from Member States. Concretely, this investment will support activities such as the setting up of advanced **pilot production lines** to accelerate innovation and technology development, the development of a cloud-based **design platform**, the establishment of **competence centres**, the development of **quantum chips**, as well as the creation of a **Chips Fund** to facilitate access to debt financing and equity.

- **Pillar two** – sets out the criteria to recognise and to support **Integrated Production Facilities** and **Open EU Foundries** that are first-of-a-kind facilities and that foster the security of supply and the resilience of the Union's semiconductor ecosystem.

  - The objective is to create a framework to ensure **security of supply** by attracting **investments** and enhancing **production capacities** in semiconductor manufacturing.

  - The recognition by the Commission as Integrated Production Facilities or Open EU Foundries allows **prioritised access to pilot lines** set up under the proposed Chips for Europe Initiative, under certain conditions.

- **Pillar three** – sets up a **coordination mechanism** between the Member States and the Commission for **monitoring the supply of semiconductors and crisis response** to semiconductor shortages.

  - The coordination mechanism between the Member States and the Commission seeks to strengthen **collaboration in monitoring the supply** of semiconductors, estimating demand, anticipating shortages, and, if necessary, triggering the activation of a crisis stage.

  - A **European Semiconductor Board**, composed of representatives of the Member States and chaired by the Commission, is established to facilitate a smooth, effective and harmonised implementation of the Chips Act, as well as assistance and advice on issues like monitoring and crisis response.

The Chips Act came into force on the **21st of September 2023**.[66]

The Cybersecurity Directive (NIS 2)

The NIS2 Directive,[67] [68] [69] formally the Directive on **measures for a high common level of cybersecurity across the Union**, was presented by the European Commission in **December 2020**, in order to update its predecessor, the NIS Directive (the first EU cybersecurity law). The proposed revision came in the face of **new cybersecurity and resilience challenges and risks** that became increasingly apparent during the pandemic, such as the **expanded cybersecurity threat landscape** in the face of the acceleration of the digital transformation, or the vulnerability of our increasingly interdependent societies in the face of unexpected risks as the pandemic proved.[68] [69]

The Commission identified several **deficiencies** that made revising the NIS Directive necessary:

- Insufficient levels of cyber resilience of businesses operating in the EU.

- Inconsistent resilience across Member States and sectors.

- Insufficient common understanding of the main threats and challenges among Member States.

- Lack of joint crisis response.

Consequently, these factors spurred the Commission to **propose a revision of the NIS Directive** to **expand the scope of cybersecurity rules** to new sectors and entities, and therefore **improve the resilience and crisis response capacities** of public and private entities.[68] The Directive came into force in **January 2023**, and Member States have until **October 2024 to transpose** the Directive.

NIS2 establishes measures to achieve a "**high common level of cybersecurity across the Union**", including the following:[67]

- **Expands the scope** of the previous Directive by **adding new sectors** based on their degree of digitalisation and interconnectedness and how crucial they are for the economy and society, while establishing a threshold rule whereby all medium and large-sized companies in selected sectors are within the scope of the Directive.

  - Sectors defined as **critical sectors** include energy, transport, banking and financial market infrastructures, health, water, digital infrastructure, ICT managed services, space, and public administration.

- "**Other critical sectors**" include postal and courier services, waste management, chemicals, food, manufacturing, digital providers, and research organisations.

- Establishes **obligations that require Member States to adopt national cybersecurity strategies** that provides for the strategic objectives, the resources required to achieve those objectives, and appropriate policy and regulatory measures, with a view to achieving and maintaining a high level of cybersecurity. The national cybersecurity strategy shall include:
  - a governance framework clarifying the roles and responsibilities for relevant stakeholders at the national level.
  - policy addressing the security of supply chains.
  - policy on managing vulnerabilities.
  - policy on promoting and developing education and training on cybersecurity.
  - measures to improve cybersecurity awareness among citizens.
- **Obligation for governments to designate or establish** competent authorities, cyber crisis management authorities, single points of contact on cybersecurity, and computer security incident response teams (CSIRTs).
  - CSIRTs provide technical assistance to entities, including by monitoring and analysing cyber threats, vulnerabilities, and incidents at the national level; providing early warnings, alerts, announcements and information on cyber threats, vulnerabilities and incidents; responding to incidents and providing assistance; or collecting and analysing forensic data and providing dynamic risk and incident analysis and situational awareness on cybersecurity.
- **Cybersecurity risk-management measures and reporting obligations** for entities, including for those identified as critical entities.
  - The Directive includes a list of 10 key elements that all companies have to address or implement as part of the measures they take, including incident handling, supply chain security, vulnerability handling and disclosure, the use of cryptography and where appropriate, encryption.
- Rules and obligations on cybersecurity **information sharing**.
  - Entities must notify their CSIRT or relevant authority of any incident that can cause or is capable of causing severe operational disruption or financial loss for the entity; or that has affected or could affect others by causing considerable material or non-material damage.
- **Supervisory and enforcement obligations** on Member States.

3.3 FUTURE LEGISLATIVE DEVELOPMENTS

As the preceding section has shown, the European Union is undertaking **intense regulatory activity** in the domain of the digital economy. As the tables at the start of subsection 3.2 showed, there are numerous Proposals for Regulations currently undergoing the legislative process in the Parliament and the Council, as well as other proposals that have been announced by the European Commission.

There are **three Proposals for Regulations** that are particularly important due to the profound impact they will have on digital economy and Big Tech companies, and which are currently undergoing the legislative procedure.

These 3 policies are:

- The Artificial Intelligence Act.
- The Data Act.
- The Cyber Resilience Act.

The Artificial Intelligence Act (AI Act)

The Artificial Intelligence Act, [18] [19] [70] [71] (formally the Proposal for a Regulation laying down harmonised rules on artificial intelligence), was presented by the European Commission in **April 2021**. Conscious of the huge **socioeconomic potential of this technology** but also its **risks for fundamental right**s, the EU has aspired to take the **global lead in regulating AI** with its ambitious Proposal for a Regulation.[1] With their concerns about unregulated AI in mind, the Commission presented the AI Act, which has several objectives under the overarching framework of **ensuring the protection of fundamental rights** and establishing a "**risk-based**" and "**human-centric**" approach to regulate AI. Specifically, the **4 objectives** of the Proposal for a Regulation are the following:

- ensure that AI systems placed on the Union market and used are **safe** and respect existing law on **fundamental rights and EU values**.
- ensure **legal certainty** to facilitate investment and innovation in AI.
- enhance **governance and effective enforcement of existing law** on fundamental rights and safety requirements applicable to AI systems.
- facilitate the **development of a single marke**t for lawful, safe and trustworthy AI applications and prevent market fragmentation.

AI systems are defined by the Proposal for a Regulation as software that are developed with techniques and approaches including machine-learning, logic and knowledge-based approaches, or statistical approaches, and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.

In this regard, the AI Act establishes:

- **harmonised rules** for the placing on the market, the putting into service and the use of artificial intelligence systems in the EU.
- **prohibitions** of certain artificial intelligence practices.
- **specific requirements** for high-risk AI systems and obligations for operators of such systems.
- **harmonised transparency rules** for AI systems intended to interact with natural persons, emotion recognition systems and biometric categorisation systems, and AI systems used to generate or manipulate image, audio or video content.
- rules on market **monitoring and surveillance**.

The **AI Act's risk-based approach** subdivides AI applications and practices into **four categories** depending on the level of risk that they create, and accordingly establishes **obligations and prohibitions** for each category:

- **Unacceptable risk AI**: the placing on the market, putting into service or use of these AI practices or systems is prohibited because they are "**tools for manipulative, exploitative and social control practices**" that **violate fundamental rights**. This includes:
  - AI systems that deploy **subliminal techniques beyond a person's consciousness** in order to **materially distort a person's behaviour** in a manner that causes or is likely to cause that person or another person physical or psychological harm.
  - AI systems that **exploit any of the vulnerabilities of a specific group** of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person physical or psychological harm.
  - AI systems used by **public authorities** or on their behalf for the **evaluation** or **classification** of the trustworthiness of natural persons (**social scoring**).
  - The use of **'real-time' remote biometric identification systems** in publicly accessible spaces for the purpose of **law enforcement**, except for under certain extraordinary circumstances and with certain safeguards.
- **High-risk AI**: this category covers AI systems that create a **high risk to people's health and safety or fundamental rights**.
  - This category includes **biometric identification and categorisation** of natural persons, AI systems used as safety components in the management and operation of critical infrastructure, AI systems used in education and vocational training, AI systems used for employment and workers management, AI systems for access to private services and public services and benefits, or AI systems used in law enforcement.
  - Due to their high-risk, the AI Act establishes **obligations for these AI systems**, including the establishment of a risk management system throughout the entire lifecycle of the AI system, technical documentation, record-keeping, transparency and provision of information to users, human oversight, or accuracy, robustness and cybersecurity.
  - Before placing high-risk AI systems on the market or into service, providers are obliged to subject it to **a conformity assessment procedure** to demonstrate that the system complies with the mandatory requirements for trustworthy AI (e.g. data quality, documentation and traceability, transparency, human oversight, accuracy and robustness). Providers of high-risk AI systems will also have to implement **quality and risk management systems**.
- **Low-risk AI**: for AI systems that are low-risk, while **no prohibitions** are imposed, certain specific **transparency requirements** apply to them.
  - Transparency obligations will apply for systems that interact with humans, are used to detect emotions or determine association with (social) categories based on biometric data, or generate or manipulate content ('deep fakes').
  - AI systems that interact with people, or their emotions or characteristics are recognised through

automated means, are obliged to inform people of that circumstance.

  - Similarly, if AI systems are used to generate or manipulate image, audio or video content that appreciably resembles authentic content, there is an obligation to disclose that the content is generated through automated means, to allow people to make informed choices or step back.

  - For instance, Generative AI systems such as ChatGPT will be obliged to comply with transparency requirements such as disclosing that the content was generated by AI, designing the model to prevent it from generating illegal content, and publishing summaries of copyrighted data used for training.

- **Minimal risk AI**: all other AI systems can be developed and used subject to the existing legislation **without additional legal obligations**.

  - The vast majority of AI systems currently used in the EU fall into this category.

  - Providers of those systems may voluntarily choose to apply the requirements for trustworthy AI and adhere to voluntary codes of conduct.

In terms of **enforcement**, the Proposed Regulation establishes that **Member States** should hold a key role in the application and enforcement of this Regulation. In this respect, each Member State should designate one or more **national competent authorities** to supervise the application and implementation, as well as carry out market surveillance activities.

Furthermore, Member States are required to designate a **national supervisory authority** to increase efficiency and set an official point of contact with the public and other counterparts, which would also represent the Member State in the **European Artificial Intelligence Board**.

The European Artificial Intelligence Board, in turn, would comprise high-level representatives of competent national supervisory authorities, the **European Data Protection Supervisor**, and the **Commission**. Its role will be to facilitate a smooth, effective, and harmonised implementation of the new AI Regulation, as well as issuing recommendations and opinions to the Commission regarding high-risk AI systems and on other aspects relevant for the effective and uniform implementation of the new rules.

In terms of **penalties for infringement**, if AI systems are put on the market or in use and don't respect the Act's requirements, the Proposal for a Regulation obliges Member States to lay down effective, proportionate and dissuasive penalties, and communicate them to the Commission.

The Regulation sets out the following thresholds to be taken into account for penalties:

- Up to €30m or 6% of the total worldwide annual turnover of the preceding financial year (whichever is higher) for infringements on prohibited practices or noncompliance related to requirements on data.

- Up to €20m or 4% of the total worldwide annual turnover of the preceding financial year for non-compliance with any of the other requirements or obligations of the Regulation.

- Up to €10m or 2% of the total worldwide annual turnover of the preceding financial year for the supply of incorrect, incomplete or misleading information to notified bodies and national competent authorities in reply to a request.

The **Council** of the European Union adopted its '**general approach**' (its negotiating position) in **December 2022**.[70] More recently, in **June 2023**, the **European Parliament** adopted its **negotiating position** on the AI Act, on the basis of which negotiations ('**trilogues**') with the Council were able to begin. The Parliament has stated that "the aim is to reach an agreement by the end of this year".[73]

The Data Act

The Data Act [72] [73] [74] [75] [76] is a Proposal for a Regulation that was presented by the European Commission in **February 2020**, as one of the two legislative initiatives under the '**European Strategy for data**' [64] a package that aims to **create a single market for data** to ensure the European Union's global competitiveness and data sovereignty.

The Data Act seeks to **boost the EU's data economy by unlocking industrial data**, optimising its accessibility and use, and fostering a **competitive and reliable European cloud market**, to "ensure that the **benefits of the digital revolution are shared by everyone**". Therefore, the Data Act seeks to **remove barriers to access data**, for both private and public sector bodies, while preserving **incentives to invest in data generation** by ensuring a balanced control over the data for its creators,

In this regard, the Data Act seeks to establish **harmonised rules on making data generated by the use of a product or related service available to the user of that product or service**, on the making data available by **data holders to data recipients**, and on the making data available by data holders to **public sector bodies or EU institutions**, agencies or bodies, where there is an exceptional need, for the performance of a task carried out in the public interest.

These rules would **apply to**:

- Manufacturers of products and suppliers of related services placed on the market in the EU and the users of such products or services.

- Data holders that make data available to data recipients in the EU.

- Data recipients in the EU to whom data are made available.

- Public sector bodies and EU institutions, agencies or bodies that request data holders to make data available where there is an exceptional need to that data for the performance of a task carried out in the public interest and the data holders that provide those data in response to such request.

- Providers of data processing services offering such services to customers in the EU.

These are some of the provisions of the Proposal for a Regulation:

- Measures that enable users of connected devices to **access the data generated by these devices and by services related to these devices**. Users would be able to share such data with third parties, boosting aftermarket services and innovation. Simultaneously, manufacturers remain incentivised to invest in high-quality data generation while their trade secrets remain protected.

- Measures to **rebalance negotiation power for SMEs and provide protection from unfair contractual terms** that are unilaterally imposed. These aim to safeguard EU companies from unjust agreements, fostering fair negotiations and enabling SMEs to participate more confidently in the digital marketplace.

- Mechanisms for **public sector bodies to access and use data held by the private sector in cases of public emergencies** such as floods and wildfires, or when implementing a legal mandate where the required data is not readily available through other means.

- New rules that grant **customers the freedom to switch between various cloud data-processing service providers**. These rules aim to promote competition and choice in the market while preventing vendor lock-in. Additionally, the Data Act includes safeguards against unlawful data transfers, ensuring a more reliable and secure data-processing environment.

- Measures to promote the **development of interoperability standards for data-sharing and data processing**, in line with the EU Standardisation Strategy.

The European **Parliament** and the **Council** of the European Union reached a **political agreement** on the Data Act in **June 2023**. The next hurdle was the formal approval of the political agreement by both co-legislators. The **Parliament** voted to adopt the legislation in **November 2023**, which means that the final step is the Council's formal approval. After its adoption, the Data Act will enter into force on the 20th day following its publication in the Official Journal and will become applicable 20 months after the entry into force.[76]

The Cyber Resilience Act

The Cyber Resilience Act [77] [78] (formally the Proposal for a Regulation on **horizontal cybersecurity requirements for products with digital elements** and amending Regulation 2019/1020) [21] [22] was proposed by the European Commission in **September 2022**.

It seeks to **bolster cybersecurity rules to ensure more secure hardware and software products**, and thus address gaps in existing legislation.

In this regard, the Act has **two broad objectives**:

- To create conditions for the development of **secure products with digital elements** by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and that manufactures take security seriously throughout a product's life cycle.

- To create conditions allowing **users to take cybersecurity into account** when selecting and using products with digital elements.

To this end, the Proposal for a Regulation establishes:

- Rules for the placing on the market of **products with digital elements** to ensure the **cybersecurity** of such products.

- **Essential requirements for the design, development and production** of products with digital elements, and **obligations for economic operators** in relation to these products with respect to cybersecurity.

- Essential requirements for the **vulnerability handling processes** put in place by manufacturers to ensure the cybersecurity of products with digital elements during the whole life cycle, and obligations for economic operators in relation to these processes.

- Rules on **market surveillance and enforcement** of the above-mentioned rules and requirements.

The **Council** of the European Union adopted its common position on the Cyber Resilience Act in **July 2023**, adopting several amendments in relation to the Act's scope and reporting obligations for instance.[79] The adoption of the general approach enabled the Council to enter into negotiations with the European Parliament.

For its part, the European **Parliament** confirmed in **September 2023** the decision of the Committee on Industry, Research and Energy to enter into **interinstitutional negotiations**. At the end of that month, co-legislators started '**trilogue**' negotiations in **September 2023** [80] to reach an agreement on the final text.

4

THE BATTLE BETWEEN THE EUROPEAN UNION AND BIG TECH COMPANIES

Within the context of this regulatory framework, the European Union has been engaged in intense **regulatory 'battles' against Big Tech companies**, especially American and Chinese ones, in an effort **to rein in these companies** and fulfil the policy imperatives outlined in section 2 (protection of individual and collective rights, defending a social market economy, preventing the fragmentation of the Single Market, and geopolitical considerations related to national security and the EU's quest for strategic autonomy and global influence).

4.1 AMERICAN BIG TECH COMPANIES

With regard to **American Big Tech companies**, the regulatory battles between the EU and Big Techs have mainly centred around **4 issues**: **data privacy, fair competition, taxation, and content moderation**. On all four issues, **the Commission has been leveraging its legislation and regulatory powers to rein in American Big Tech companies**. Indeed, the EU's assertive digital regulatory approach has imposed significant **constraints on American Big Tech companies**, and has brought them into protracted battles with the EU, at times involving the US government itself as it has sought to "come to the rescue" its Big Tech companies.[1]

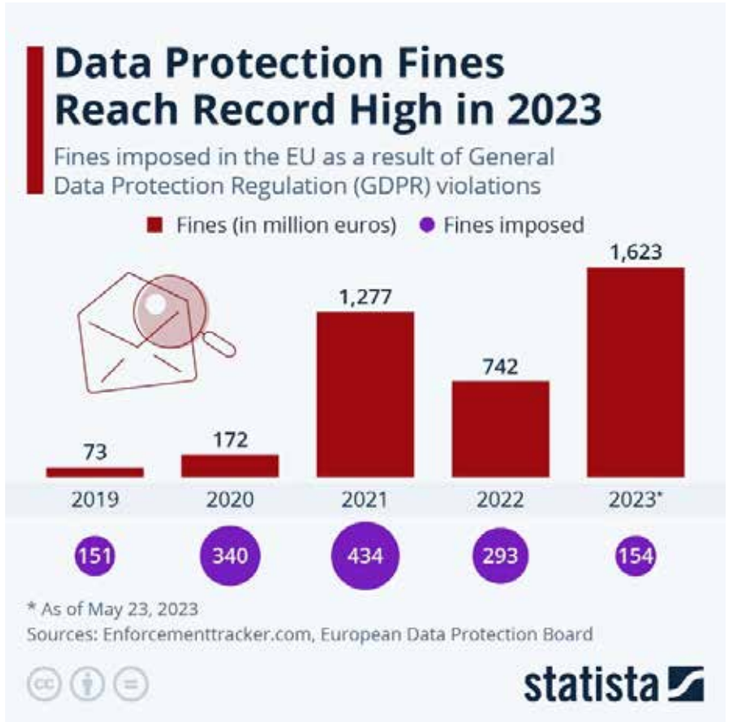
Part of the cause of the regulatory clash between the EU and Big Techs is undoubtedly the **different approaches of the EU and US regulatory models**, in the sense that, as section 2 analysed, the EU believes it must leverage regulations to **protect Europeans' fundamental rights being violated by Big Tech companies' business practices**, to rein in Big Tech companies that **exploit their market power**, and ensure a fair, competitive market; in contrast to the USA's regulatory model of **free markets and limited government intervention**, which leads America to view the EU's regulatory actions as "**regulatory overreach**" and "**protectionism**", unfairly targeting American companies. This clash is best epitomised by the EU's response to Elon Musk's acquisition of Twitter in 2022. After his acquisition, Musk tweeted "the bird has been freed", to which the European Commissioner for Internal Market, Thierry Breton, replied: "**In Europe, the bird will fly by our rules**".[81]

However, the USA's support for limited government intervention also follows a **geopolitical logic**, as the **source of America's global influence** in the digital sphere is its "**private power**", embodied by the **dominance of its Big Tech companies**.[1] On the other side of the coin, the EU's regulatory zeal against (mainly US) Big Tech companies arguably also follows a geopolitical imperative. As the last section explained, the EU is increasingly concerned, and arguably also resentful, about the **USA's dominance in the digital economy and the perceived abuse of its dominant position**, and these concerns may be **feeding into the EU's regulatory actions** against American Big Tech companies.[29]

On **data privacy**, the battle between the European Union (EU) and American Big Tech companies has been characterised by a **clash of regulatory philosophies** and divergent approaches to safeguarding individuals' privacy rights. At the forefront of this conflict stands the implementation of the General Data Protection Regulation (**GDPR**) and the obligations it imposes on Big Tech companies in relation to treatment of persona data. Specifically, regulatory clashes have centred on two broad issues: firstly, on **private companies' extraction and monetisation of users' personal data**, and secondly, **protection of private data from government surveillance**. In contrast to the EU's extensive protection of data privacy, in the USA, data is a "commodity" that can be monetised by Big Tech companies with few restrictions, while the US government has greater authority to engage in digital surveillance on the grounds of national security,[1] as was exposed in scandals such as the **Snowden revelations**.[10]

As a result of these competing visions, the clash between the EU and Big Techs is based on the fact that **the European Union imposes regulatory constraints on these companies** the likes of which they don't face in the USA. These stem from the EU's twofold concerns: firstly, the concern that US **Big Tech companies' business practices undermine fundamental rights** like data privacy, and secondly concerns that **personal data isn't sufficiently protected from US government surveillance**.[1] In this regard, there are numerous examples of the regulatory battles between the EU and Big Techs.

For example, in **July 2021**, **Luxembourg's National Commission for Data Protection** (CNPD) imposed a **€746 million fine on Amazon** for processing personal data in violation of the EU's GDPR rules.[82] [83] More recently and more substantially, in **May 2023**, **Ireland's Data Protection Commission** (DPC), which is responsible for regulating Meta across the EU, **fined Meta €1.2 billion** for continuing to **transfer personal data of EU users to the USA** in a way that "**did not address the risks to the fundamental rights and freedoms of data subjects** that were identified" by the European Court of Justice's 2020 ***Schrems II* judgement**,[84] which struck down the EU-US Privacy shield governing transatlantic data transfers on the grounds of concerns about US surveillance, and upheld that companies can continue to transfer data through standard contractual clauses (**SCCs**) if they provide "**appropriate data protection safeguards**".[185] As a result of the DPC's ruling, Meta was ordered to **suspend the transfer of user data from the EU to the US** within 5 months, and to stop within 6 months the "unlawful processing, including storage, in the US" of data already transferred to the USA.[84]



Source: Statista

Big Tech companies have **rhetorically and legally retaliated against the EU**. Amazon denounced the CNPD ruling to be "without merit" and assured they would defend themselves "vigorously". On their part, Meta denounced the DPC's ruling as "unjustified and unnecessary", and has stated that they will **appeal against it**.[83] In fact, **Meta** has warned that it may be "**unable to offer a number of our most significant products and services**, including Facebook and Instagram, in Europe" if no solution is found for **transatlantic data transfers**.[84]

There is some hope that these regulatory battles may be resolved, as the **USA government** has gotten involved to "**come to the rescue of its companies**".[1] And despite the persistent thorns in transatlantic relations that data transfers have supposed, this battle seems to be on path towards a resolution and greater regulatory alignment. In **March 2022**, Commission President Ursula von der Leyen and US President Joe Biden reached a **preliminary deal on a new EU-US Data Privacy Framework** to implement safeguards that would enable to restore transatlantic data flows. In **October 2022**, Biden signed an **Executive Order** to implement the agreement into law, while more recently in **July 2023** the **European Commission adopted an adequacy decision** concluding that the **US ensures an adequate level of protection for personal** data transferred from the EU, on the basis of the Data Privacy Framework agreed.[86] [87] Nonetheless, there are no guarantees that the agreement won't be **challenged in the courts**.

Another front on which the EU has fought regulatory battles against Big Tech companies is **competition policy**, whereby the EU has sought to **leverage its regulatory powers against US Big Tech companies that allegedly exploit their market power and undermine a competitive marketplace**. Indeed, these regulatory battles are underpinned by the fundamentally **"asymmetrical" nature of the EU-US relationship** in the digital economy (as section 3 explained): while the EU

resents US Big Tech companies' dominant position and anticompetitive practices, US Big Tech companies and indeed also the US government resent the EU's stringent competition policy enforcement, which they perceive as "protectionist" and **deliberately targeting innovative US Big Tech companies**.[1]

Examples include the EU's **€2.42 billion fine against Google in 2017** for breaching EU antitrust rules, specifically "**abusing its market dominance** as a search engine by giving an **illegal advantage to another Google product**, its comparison shopping service".[88] The EU once again imposed a **€4.34 billion fine against Google in 2018** for imposing "**illegal restrictions on Android** device manufacturers and mobile network operators to **cement its dominant position** in general internet search".[89] Furthermore, in **2022**, the Commission issued a **preliminary view to Facebook**, finding that the company had company **breached EU antitrust rules by distorting competition in the markets for online classified ads**.[90] And most recently, the EU adopted the **Digital Markets Act**, which as section 3 explained, will prohibit Big Tech companies (including US tech giants Amazon, Apple, Google, Meta and Microsoft), from engaging in **uncompetitive business practices**.[1]

Indeed, as with data privacy, the **US government** has gotten involved on the side of American Big Tech companies, **accusing the EU of regulatory overreach and protectionism**.[1] As President **Obama** asserted in 2015, "oftentimes what is portrayed as high-minded positions on issues", in reference to the European Union's regulatory oversight, "sometimes is just designed to **carve out some of their commercial interests**".[91] Big Tech companies have also **fought back** against the EU's competition policy. For instance, several of the Big Tech companies who were **designated as "gatekeepers under the DMA** have filed **legal challenges** against the Commission's designation decisions, including Meta and TikTok; while Amazon challenged its designation as a Very Large Online Platform under the Digital Services Act.[92] Meta and Google have taken things further. Meta has announced that its social media platform **Threads** (a rival to Twitter) will **not be available in the EU**, while the same is true for Google's **Bard** (a rival to OpenAI's ChatGPT), allegedly due to "**regulatory uncertainty**", or what POLITICO describes as a "**canny lobbying tactic** just as Brussels is finishing separate antitrust [the DMA] and artificial intelligence [the AI Act] rules that will directly target" these Big Techs.[93]

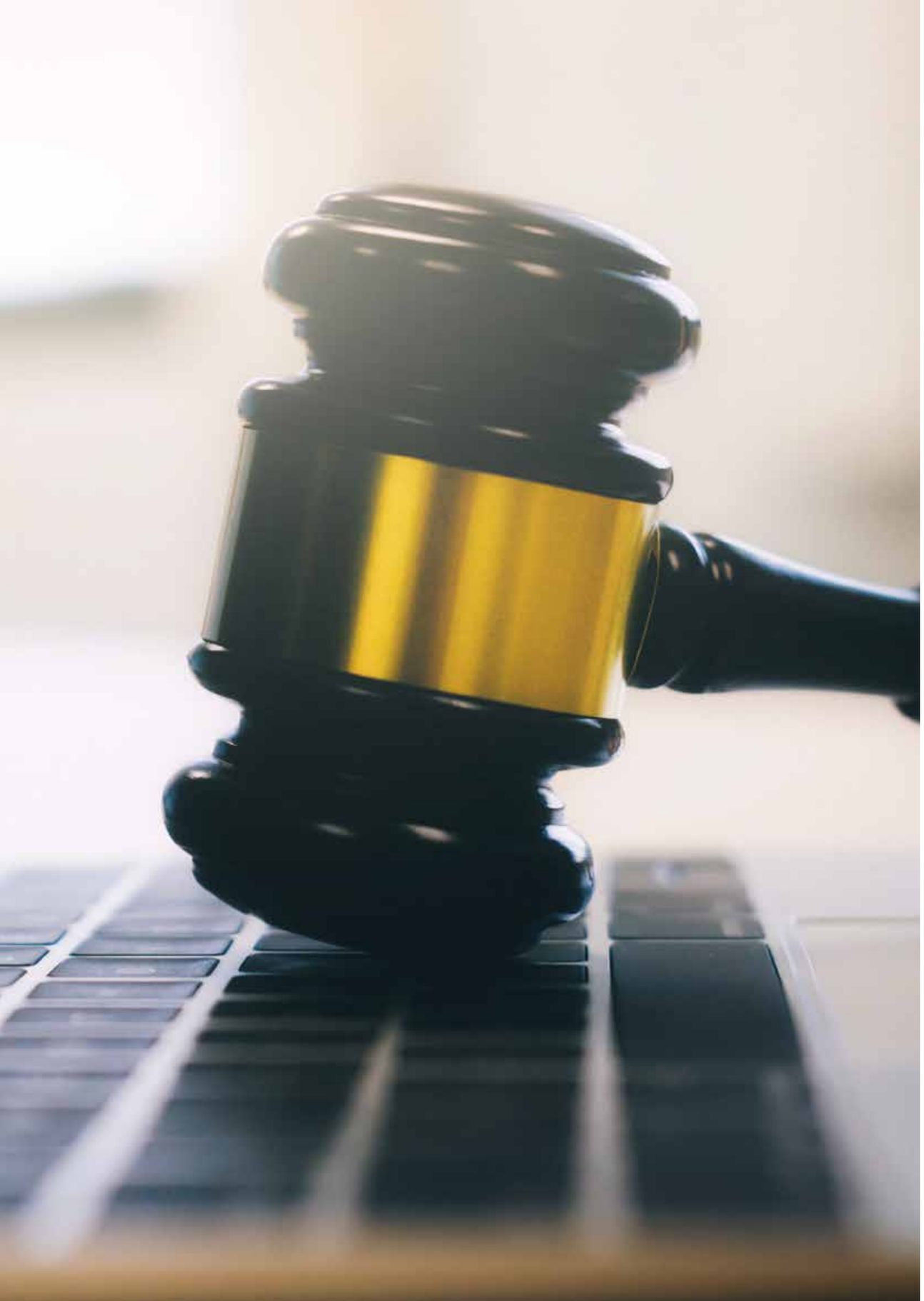
However, whether Meta and Google will ultimately follow through with this decision and **forgo access to the lucrative EU Single Market** remains to be seen. And in fact, other companies like Microsoft and Amazon have manifested their willingness to **comply and work constructively** with the EU.[92] In fact, in the face of the **EU's vast regulatory apparatus**, there is very little that Big Tech companies can do if they do not want to forgo access to the EU's market. **US Big Techs invest very heavily in lobbying activities in Brussels** (indeed aware that the Brussels Effect can give lobbyists a say not only about EU but global regulation), but nonetheless, in Brussels, business interests are no more influential in shaping EU regulations than other interests, meaning that lobbying efforts by Big Techs have done "**little to rein in the European regulators**".[1] Instead, Big Tech companies have largely been forced to "**concede that the EU will regulate them**" and focus their legal efforts on compliance.[1]

However, the EU's regulatory battles against Big Tech companies haven't been confined to American Big Techs. Although battles between the EU and **Chinese Big Tech companies** have been less numerous and less prominent, there have also been a number of them in the last years. As with US Big Techs, the EU's regulatory battles with the Chinese Big Techs have also surrounded **concerns about data privacy and other economic issues** related to these companies' business practices and the Chinese state's unfair practices, but unlike with American Big Techs, there have also been important considerations related to **national security** in the case of regulatory battles with Chinese Big Techs, as was broadly outlined in subsection 2.2 on the EU's geopolitical considerations.

For example, in his November 2023 speech in Beijing, the EU's Commissioner for Internal Market, **Thierry Breton**, expressed concerns about the **Chinese state's unfair practices**. Breton highlighted that "**competition needs to take place on fair and reciprocal terms, not by dumping products on markets, keeping prices artificially low with state subsidies, or favouring domestic manufacturers over European operators**", and that in this regard, Europe would "take action when warranted to safeguard our interests", including by launching an "anti-subsidies investigation into electric vehicles coming from China to establish whether anticompetitive behaviour is taking place, and if so, to act upon it".[36] Furthermore, in **September 2023 TikTok was fined €345 million** by the Irish Data Protection Commission (DPC) for **multiple breaches of the GDPR in its handling of children's accounts**, including placing child users' accounts on a public setting by default, failing to supply transparent information to child users, allowing an adult accessing a child's account on the "family pairing" setting to enable direct messaging for over-16s, and not properly taking into account the risks posed to under-13s on the platform who were placed on a public setting.[94]

However, with TikTok and indeed other Chinese Big Techs, **the EU's regulatory concerns about data privacy have also incorporated an important national security element**, due to the **authoritarian nature of the Chinese state and the geopolitical concerns** that were analysed in subsection 2.2. For instance, in **February 2023**, the European **Commission** decided to "**suspend the use of the TikTok application on its corporate devices** and on personal devices enrolled in the Commission mobile device service … to **protect the Commission against cybersecurity threats** and actions which may be exploited for cyber-attacks against the corporate environment of the Commission".[95] Although the Commission didn't mention China by name, the policy move was a result of growing **fears that sensitive personal data controlled by Chinese Big Tech companies could be directly accessed by the Chinese Communist Party** for purposes like focusing on political targets, and in fact, Ireland's Data Protection Commission (DPC) has been investigating TikTok's data transfers to China since 2021.[96]

Other Chinese Big Tech companies like **Huawei** have also been caught up in the mix of the EU's regulatory battles for national security reasons. As was outlined in subsection 2.2, there have been **concerns in the EU about the national security risks posed by relying on Huawei providing 5G infrastructure**. In **June 2023**, the European Union Member States, with the support of the European Commission and the EU Agency for Cybersecurity, published a second **progress report** on the implementation of the **EU Toolbox on 5G cybersecurity**, while in parallel to the progress report, the **European Commission** adopted a **Communication** on the implementation of the toolbox. In this Communication, the European Commission asserted that it "**considers that decisions adopted by Member States to restrict or exclude Huawei and ZTE from 5G networks are justified and compliant with the 5G Toolbox**", and that indeed the Commission "**considers that Huawei and ZTE represent in fact materially higher risks than other 5G suppliers**". On this basis, the recommendation formulated for Member States is that "based on the assessment of suppliers", they "**impose restrictions on high-risk suppliers without delay**, i.e. considering that a loss of time can increase vulnerability of networks in the Union and the Union's dependency on high-risk suppliers, especially for Member States with a high presence of potential high-risk suppliers".[97]



7

CONCLUSION

In conclusion, as this report has shown, **the European Union has become a crucial (and global) battleground for Big Tech companies** for two broad reasons.

Firstly, because **the European Union is a powerful and stringent regulator of Big Techs** and of the digital economy. As a result of **diverse policy imperatives**, such as integration of the European Single Market, protecting EU citizens' fundamental rights, preserving democracy, ensuring a fair and competitive social market economy, and more recently, preserving Europe's strategic autonomy and digital sovereignty, **the European Union has enacted a comprehensive web of legislation and regulations** governing the Digital Economy.

The **key legislation and regulations** that the European Union has enacted have had a **significant impact on these corporations** due to the costs and obligations that they impose. Big Tech companies have attempted to **fight back against these regulations**, including through intense lobbying, but at all times, Big Tech companies have had to reconcile their business interests with the fact that the EU is a large and attractive market for their products and their service. Ultimately, **Big Tech companies have been forced to either comply with the EU's stringent regulations, or forgo access to the EU market**, with most Big Techs having opted for the former.

The second interrelated reason why the European Union has become a battleground for Big Techs is the **'Brussels Effect'**. As this report has thoroughly analysed, **the European Union's regulatory activity transcends its own borders** and has an **impact on companies and governments around the world**, and this also applies to the digital sphere. For this reason, the **regulatory developments that take place in the European Union are of great interest and can have a huge impact on Big Tech companies and their global operations**, as this report has explained through its detailed analysis and examples.

Nevertheless, **the European Union will continue to face challenges in regulating Big Techs going forward**. The EU will have to continue to navigate the complexities of regulating rapidly advancing technologies such as artificial intelligence while ensuring **consistent enforcement** across Member States, and also **balancing innovation with regulation**. But no doubt, as the digital transformation progresses and digital technologies become even more pervasive in all aspects of life and the economy, **the European Union will continue to intensely regulate Big Techs to ensure that the digital economy conforms to European values**, and the rights and welfare of its citizens.

Furthermore, as the report has highlighted, as **geopolitical considerations become more salient**, they will **increasingly shape the EU's digital regulations**, as technological competition will increasingly become embedded between the broader global dynamics of geopolitical competition. In its quest for digital sovereignty and the ability to compete geopolitically, **the lack of any European Big Tech companies will likely remain a challenge for the EU and an impediment in its quest to become a digital superpower in its own right**, rather than just a hegemonic regulator.

REFERENCES:

1. Anu Bradford (2023), 'Digital Empires: The Global Battle to Regulate Technology' (Oxford University Press)

2. Anu Bradford (2020), 'The Brussels Effect: How the European Union Rules the World' (Oxford University Press)

3. 'Why big tech should fear Europe' (The Economist)

4. Andrés Ortega Klein (2020), 'The view from Spain: The EU's bid for digital sovereignty', in 'Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry (European Council on Foreign Relations)

5. Jeremy Shapiro (2020), 'Introduction: Europe's Digital Sovereignty', in 'Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry (European Council on Foreign Relations)

6. Ewen MacAskill (2023), 'The Snowden Revelations Reconsidered' (The Atlantic)

7. Nicholas Confessore (2018), 'Cambridge Analytica and Facebook: The Scandal and the Fallout So Far' (The New York Times)

8. Andrew Puddephatt (2020), 'Governing the internet: The makings of an EU model', in 'Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry (European Council on Foreign Relations)

9. Anu Bradford (2023), 'Europe's Digital Constitution' (Virginia Journal of International Law)

10. McKinsey Global Institute (2019), 'Innovation in Europe: Changing the game to regain a competitive edge' (McKinsey & Company)

11. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Agenda for Europe (EUR-Lex)

12. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (European Commission)

13. 'Shaping Europe's Digital Future' (European Commission)

14. European Declaration on Digital Rights and Principles for the Digital Decade (European Commission, Parliament and Council of the EU)

15. Josep Borrell and Margrethe Vestager (2021), 'Why Europe's Digital Decade Matters' (European Union External Action)

16. Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (EUR-Lex)

17. Ethics Guidelines for Trustworthy AI (European Commission)

18. Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts) (EUR-Lex)

19. EU AI Act: first regulation on artificial intelligence (European Parliament)

20. President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence (The White House)

21. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (EUR-Lex)

22. Proposal for a Regulation of the European Parliament and of the Council on the transparency and targeting of political advertising (EUR-Lex)

23. Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (European Commission)

24. Commission staff working document – The external dimension of the single market review – Accompanying document to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A single market for 21st century Europe (EUR-Lex)

25. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions – A single market for citizens (EUR-Lex)

26. Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – A comprehensive approach on personal data protection in the European Union (EUR-Lex)

27. State of the Union Address by President von der Leyen at the European Parliament Plenary (European Commission)

28. 2023 State of the Union Address by President von der Leyen (European Commission)

29. Mark Zuckerberg (2019), 'Mark Zuckerberg: The Internet needs new rules. Let's start in these four areas' (The Washington Post)

30. Online Safety Act (UK Parliament)

31. Digital Markets, Competition and Consumers Bill (UK Parliament)

32. Kate Beioley and Jim Pickard (2023), 'UK set to legislate to create new regulator to tackle Big Tech' (Financial Times)

33. EU Strategic Autonomy Monitor (2022), 'EU strategic autonomy 2013-2023: From concept to capacity' (European Parliament)

34. Open Strategic Autonomy for a competitive and resilient EU (Spanish Presidency of the Council of the EU)

35. Josep Borrell (2020), 'Why European strategic autonomy matters' (European Union External Action)

36. 'In the geopolitics of blocs, Europe as a power of balance – Speech by Commissioner Breton (European Commission)

37. Raluca Csernatoni (2021), 'The EU's Rise as a Defence Technological Power: From Strategic Autonomy to Technological Sovereignty' (Carnegie Europe)

38. Remarks by President Biden on the American Jobs Plan (The White House)

39. El impacto de la Inflation Reduction Act en las relaciones transatlánticas (Real Instituto Elcano)

40. EU-China Relations factsheet – April 2022 (European Union External Action)

41. Assessing China's Digital Silk Road Initiative: A Transformative Approach to Technology Financing or a Danger to Freedoms? (Council on Foreign Relations)

42. EU considers mandatory ban on using Huawei to build 5G (Financial Times)

43. Informal meeting of Heads of State or Government: Versailles Declaration – 10 and 11 March 2022 (European Council)

44. 2021 State of the Union Address by President von der Leyen (European Commission)

45. Regulation (EU) 2023/1781 of the European Parliament and of the Council of 13 September 2023 establishing a framework of measures for strengthening Europe's semiconductor ecosystem and amending Regulation (EU) 2021/694 (Chips Act) (EUR-Lex)

46. Commission Recommendation of 3.10.2023 on critical technology areas for the EU's economic security for further risk assessment with Member States (European Commission)

47. EU budget: Commission proposes Strategic Technologies for Europe Platform (STEP) to support European leadership on critical technologies (European Commission)

48. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Single Market Strategy for Europe' (EUR-Lex)

49. Political Guidelines for the Next European Commission 2019-2024 (European Commission)

50. Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030 (EUR-Lex)

51. Identification and assessment of existing and draft EU legislation in the digital field (European Parliament)

52. The general data protection regulation (European Council)

53. The Digital Services Act package (European Commission)

54. The Digital Services Act: ensuring a safe and accountable online environment (European Commission)

55. Digital Services Act (European Council)

56. Questions and Answers: Digital Services Act (European Commission)

57. Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines (European Commission)

58. The Digital Markets Act: ensuring fair and open digital markets (European Commission)

59. Digital Markets Act: Commission designates six gatekeepers (European Commission)

60. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (EUR-Lex)

61. Shaping Europe's digital future: European Data Governance Act explained (European Commission)

62. European Data Governance Act (European Commission)

63. Regulation on data governance – Questions and Answers (European Commission)

64. European Strategy for data (European Commission)

65. European Chips Act enters into force today – Questions and answers (European Commission)

66. Digital sovereignty: European Chips Act enters into force today (European Commission)

67. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (EUR-Lex)

68. Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) (European Commission)

69. Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) – FAQs (European Commission)

70. Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights (Council of the EU)

71. New rules for Artificial Intelligence – Questions and Answers (European Commission)

72. Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) (European Commission)

73. Data Act: Commission welcomes political agreement on rules for a fair and innovative data economy (European Commission)

74. Data Act: Commission proposes measures for a fair and innovative data economy (European Commission)

75. Data Act – Questions and answers (European Commission)

76. Parliament backs plans for better access to, and use of, data (European Parliament)

77. Proposal for a Regulation of the Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (EUR-Lex)

78. Cyber Resilience Act (European Commission)

79. Cyber resilience act: member states agree common position on security requirements for digital products (European Council)

80. Horizontal cybersecurity requirements for products with digital elements (European Parliament)

81. 'Elon Musk's Twitter "bird will fly by EU rules," Brussels warns after billionaire takes control' (Euronews)

82. Vincent Manancourt (2021), 'With Amazon fine, Luxembourg emerges as Europe's unlikely privacy champion' (POLITICO)

83. Amazon hit with record EU data privacy fine (Reuters)

84. Dan Milmo and Lisa O'Carroll (2023), 'Facebook owner Meta fined €1.2bn for mishandling user information' (The Guardian)

85. Standard Contractual Clauses (European Commission)

86. Questions & Answers: EU-U.S. Data Privacy Framework (European Commission)

87. Questions & Answers: EU-US Data Privacy Framework (European Commission)

88. Antitrust: Commission fines Google €2.42 billion for abusing dominance as search engine by giving illegal advantage to own comparison shopping service – Factsheet (European Commission)

89. Antitrust: Commission fines Google €4.34 billion for illegal practices regarding Android mobile devices to strengthen dominance of Google's search engine (European Commission)

90. Antitrust: Commission sends Statement of Objections to Meta over abusive practices benefiting Facebook Marketplace (European Commission)

91. Obama attacks Europe over technology protectionism (Financial Times)

92. Edith Hancock (2023), 'TikTok, Meta take EU to court over digital antitrust rules' (POLITICO)

93. Mark Scott (2023), 'Europe's Big Tech rules come at a cost. Look at Threads and Bard' (POLITICO)

94. Dan Milmo (2023), 'TikTok fined €345m for breaking EU data law on children's accounts' (The Guardian)

95. Commission strengthens cybersecurity and suspends the use of TikTok on its corporate devices (European Commission)

96. Jorge Liboreiro and Natalie Huet (2023), 'European Commission bans its staff from using TikTok over China cybersecurity concerns' (Euronews)

97. Commission announces next steps on cybersecurity of 5G networks in complement to latest progress report by Member States (European Commission)

newdirection.online @europeanreform

New Direction is registered in Belgium as a not-for-profit organisation and is partly funded by the European Parliament.